Administration iQ.Suite 5 für EXCHANGE

GROUP
TECHNOLOGIES

Impressum

Alle Rechte vorbehalten. Dieses Handbuch und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der GROUP Technologies AG, Karlsruhe, Deutschland.

Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der GROUP Technologies AG zulässig.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller/Inhaber.

Copyright © 2005 GROUP Technologies AG,
Ottostrasse 4, 76227 Karlsruhe, Deutschland

Ausgabe: Januar 2005

Inhalt

1 Vorwort ... 1

1.1 Qualitätssicherung ... 1
1.2 Hotline ... 1
1.3 Ein Fehler: Was nun? ... 2
1.4 Urheberrecht ... 2
1.5 Gewährleistung ... 2
1.6 Lizenzvereinbarungen ... 3
1.7 Copyright Vermerke Dritter ... 3

2 Einleitung ... 5

2.1 Der Sinn eines Handbuchs ... 5
2.2 Aufbau dieses Handbuchs ... 5

3 E-Mail Lifecycle Management - Produktüberblick ... 7

3.1 E-Mail Pre-Processing ... 8
3.1.1 iQ.Suite Crypt ... 8
3.1.2 iQ.Suite Trust ... 9
3.1.3 iQ.Suite Trailer ... 9
3.2 E-Mail Firewall ... 10
3.2.1 iQ.Suite Watchdog ... 11
3.2.2 iQ.Suite Wall ... 12
3.3 E-Mail Classification ... 13
3.3.1 iQ.Suite Wall ... 13
3.4 E-Mail Compliance ... 14
3.4.1 iQ.Suite Bridge ... 14
3.5 E-Mail Archiving, Retrieval, Retention ... 15
3.5.1 iQ.Suite Bridge ... 15
3.6 Leistungsmerkmale aller Produkte ... 16

4 Quickstart ... 17

4.1 Installation auf einem Exchange-Server ... 17
4.2 Installation auf mehreren Exchange-Servern ... 17
4.3 Starten der iQ.Suite Konsole ... 17
4.4 Konfiguration in der iQ.Suite Konsole ... 18
4.4.1 Basis-Konfiguration ... 18
4.4.2 Richtlinien-Konfiguration ... 19
4.4.3 iQ.Suite Monitor ... 19
4.5 Notwendige Schritte nach der Installation ... 20
4.5.1 Einstellungen von iQ.Suite Servers ... 20
4.5.1.1 Gepackte Dateien und iQ.Suite Monitor ... 20
4.5.1.2 Definition der E-Mail-Adressen und internen Domänen ... 21
4.5.2 Virenscanner aktiv setzen ... 22

4.5.3 Jobs aktiv schalten 23
5 Installation 25
5.1 Systemvoraussetzungen 25
5.2 Vorbereitungen 25
5.2.1 Installation der Virenscanner 25
5.2.2 Update von iQ.Suite 3.x oder 4 auf Version 5 26
5.3 Durchführung 27
5.3.1 Installation der iQ.Suite auf einem Exchange-Server 27
5.3.2 Installation der iQ.Suite auf mehreren Exchange-Servern 31
5.3.2.1 Wissenswertes zur Installation 31
5.3.2.2 Installation der Serverkomponenten auf den Servern 33
5.3.2.3 Installation der iQ.Suite Konsole auf einer Workstation 36
5.4 Deinstallation der iQ.Suite 5 für Exchange 38
5.5 Erstinstallation für MS Active/Passive Cluster-Server 38
5.5.1 Installationsschritte 38
5.5.2 Lokale Installation der iQ.Suite 39
5.5.3 Anpassen der aktiven Knoten 40
5.5.3.1 Kopieren des GrpData- und Config-Verzeichnisses 40
5.5.3.2 Anpassen der Registry 41
5.5.3.3 Anpassen der iQ.Suite Konfigurationsdatei 42
5.5.4 Kopieren der Lizenzdateien auf alle Knoten 43
5.5.5 Einrichten der iQ.Suite als Cluster-Ressource 43
5.5.6 Aktivieren des Grabbers 49
5.5.7 Beispiel einer Erstinstallation auf einem 4-Knoten-Cluster 50
5.6 Update von V3.x/V4.0 nach V5.0 in einem Cluster 54
5.6.1 Update der passiven Knoten CLNODE1 55
5.6.2 Failover der EVS von CLNODE1 nach CLNODE2 58
5.6.3 Update des vormals aktiven Knotens CLNODE1 65
5.6.4 Fallback auf Ursprungsknoten 65
5.6.5 Beispiel eines Updates auf einem 4-Knoten Cluster 65
5.7 Deinstallation der iQ.Suite in einem Cluster 66
5.7.1 Deaktivieren des Grabbers 67
5.7.2 Warten, bis iQ.Suite Warteschlangen leer sind 67
5.7.3 Entfernen der iQ.Suite Cluster-Resource 68
5.7.4 Lokale Deinstallation auf allen Knoten 68
5.7.5 Löschen der iQ.Suite Verzeichnisse auf Disk-Resourcen 69
6 Allgemeines 71
6.1 Die iQ.Suite Architektur 71
6.1.1 Die iQ.Suite Konsole 71
6.1.2 Der iQ.Suite Server 72
6.1.2.1 Der Grabber 72
6.1.2.2 Der iQ.Suite Service = Enterprise Message Handler (EMH) 73
6.1.2.3 Die iQ.Suite Quarantäne 74

6.1.2.4 Das Active Directory / LDIF ... 75
6.1.2.5 Die Windows Registry ... 76
6.1.2.6 Komprimierte Dateien/Archive: Der iQ.Suite Entpacker ... 76
6.1.2.7 Die iQ.Suite In-Queue ... 77
6.1.3 Die iQ.Suite Konfiguration ... 78
6.2 Ablauf der E-Mail-Verarbeitung ... 79
6.3 Die Benutzeroberfläche ... 80
6.3.1 Die Symbolleiste: ... 81
6.3.2 Bedeutung der Icons ... 81
6.4 Konfiguration in der iQ.Suite Management Konsole ... 84
6.5 Basis-Konfiguration ... 85
6.5.1 Konfiguration importieren ... 85
6.5.2 iQ.Suite Servers-Einstellungen ... 85
6.5.3 Einstellungen für einen einzelnen iQ.Suite Server ... 85
6.5.3.1 Allgemeine Servereinstellungen ... 86
6.5.3.2 Individuelle E-Mail-Adressen für einen iQ.Suite Server ... 87
6.5.3.3 Benutzerspezifischer Zugriff auf die Quarantäne ... 87
6.5.3.4 Quarantänewartung ... 89
6.5.3.5 Liste aller Jobs ansehen ... 90
6.5.4 Adresslisten ... 90
6.5.4.1 Eigene Adresslisten anlegen, bearbeiten und löschen ... 90
6.5.4.2 Einsatz und Handhabung in einem Job ... 93
6.5.5 Benachrichtigungsvorlagen erstellen ... 100
6.5.5.1 Liste der Benachrichtigungsvariablen ... 101
6.5.6 Trailer ... 110
6.5.7 Ordner-Einstellungen ... 110
6.5.7.1 Quarantäne konfigurieren ... 110
6.5.7.2 Bridge ... 116
6.5.8 Utility-Einstellungen ... 116
6.5.8.1 CORE Klassifikatoren ... 116
6.5.8.2 Fingerprints ... 117
6.5.8.3 Wortlisten ... 117
6.5.8.4 Virenscanner ... 117
6.5.8.5 DCC ... 117
6.5.8.6 Crypt Engines ... 117
6.6 Richtlinien-Konfiguration ... 118
6.6.1 Beispiel einer Unternehmensrichtlinie ... 118
6.6.2 Jobtypen ... 118
6.6.3 Aktionen ... 121
6.6.4 Prioritäten der Jobs ... 122
6.7 iQ.Suite Monitor ... 123
6.7.1 Quarantänen ... 124
6.7.1.1 Beispiel einer E-Mail in der Quarantäne ... 125
6.7.1.2 Beispiel einer E-Mail in der Informationsspeicher-Quarantäne ... 128
6.7.1.3 Aus Quarantäne senden ... 130

6.7.1.4 Bad-Mails ... 132
6.7.2 CORE Klassifikatoren ... 132
6.7.3 iQ.Suite Reports ... 133
7 iQ.Suite Crypt ... 135
7.1 Übersicht ... 135
7.1.1 Jobtypen ... 136
7.1.2 Quickstart PGP/GnuPG ... 137
7.1.3 Quickstart S/MIME ... 138
7.2 PGP/GnuPG - Allgemeines ... 138
7.2.1 PGP ... 139
7.2.2 PGP/MIME ... 139
7.3 Vorbereitungen für PGP ... 140
7.4 Konfiguration der PGP bzw. GnuPG Crypt Engine ... 140
7.4.1 Beispielkonfiguration GnuPG bzw. PGP ... 141
7.4.1.1 Allgemeine Einstellungen ... 141
7.4.1.2 PGP Optionen einrichten ... 143
7.4.1.3 Fingerprints hinzufügen oder entfernen ... 144
7.4.1.4 Variablen definieren ... 145
7.4.1.5 Jobs überprüfen ... 146
7.4.1.6 Details ... 146
7.5 Automatischer Schlüsselimport mit PGP/GnuPG ... 146
7.5.1 Voraussetzungen ... 146
7.5.2 Ablauf des Schlüsselimports ... 146
7.5.3 PGP Schlüssel importieren - Jobbeispiel ... 146
7.5.3.1 Allgemeine Einstellungen ... 147
7.5.3.2 Adressbedingungen einrichten ... 148
7.5.3.3 Optionen auswählen - Crypt Engine ... 148
7.5.3.4 Aktionen festlegen ... 149
7.5.3.5 Server auswählen / Job Details ... 150
7.6 Verschlüsseln mit PGP/GnuPG ... 151
7.6.1 Voraussetzungen ... 151
7.6.2 Ablauf der Verschlüsselung mit PGP oder PGP/MIME ... 151
7.6.3 E-Mails mit PGP/GnuPG verschlüsseln - Jobbeispiel ... 151
7.6.3.1 Allgemeine Einstellungen ... 152
7.6.3.2 Adressbedingungen einrichten ... 153
7.6.3.3 Crypt Engine auswählen - Verschlüsselungsmethode ... 153
7.6.3.4 Crypt Modus auswählen - Verschlüsselungsmodus - VPN . 155
7.6.3.5 Mapping auswählen - Key ID-Zuordnung ... 158
7.6.3.6 Aktionen festlegen ... 159
7.6.3.7 Server auswählen / Job Details ... 160
7.7 Entschlüsseln mit PGP/GnuPG ... 161
7.7.1 Voraussetzungen ... 161
7.7.2 Ablauf der Entschlüsselung mit PGP oder PGP/MIME ... 161
7.7.3 E-Mails mit PGP/GnuPG entschlüsseln - Jobbeispiel ... 161
7.7.3.1 Allgemeine Einstellungen ... 162

7.7.3.2 Adressbedingungen einrichten ... 163
7.7.3.3 Crypt Engine/Modus auswählen - Methode ... 163
7.7.3.4 Aktionen festlegen ... 166
7.7.3.5 Server auswählen / Job Details ... 167
7.8 S/MIME - Allgemeines ... 167
7.8.1 Vorbereitungen für S/MIME ... 167
7.9 Konfiguration der S/MIME Crypt Engine ... 168
7.9.1 Beispielkonfiguration S/MIME ... 168
7.9.1.1 Allgemeine Einstellungen ... 168
7.9.1.2 S/MIME Optionen einrichten ... 170
7.9.1.3 Variablen ... 171
7.9.1.4 Jobs überprüfen ... 172
7.9.1.5 Details ... 172
7.10 Verschlüsseln mit S/MIME ... 172
7.10.1 Ablauf der Verschlüsselung mit S/MIME ... 172
7.10.2 E-Mails mit S/MIME verschlüsseln - Jobbeispiel ... 173
7.10.2.1Allgemeine Einstellungen ... 173
7.10.2.2Adressbedingungen einrichten ... 174
7.10.2.3Crypt Engine auswählen - Verschlüsselungsmethode ... 174
7.10.2.4Crypt Modus auswählen - Verschlüsselungsmodus - VPN ... 176
7.10.2.5Mapping auswählen - Key ID-Zuordnung ... 179
7.10.2.6Aktionen festlegen ... 180
7.10.2.7Server auswählen / Job Details ... 181
7.11 Entschlüsseln mit S/MIME ... 181
7.11.1 Ablauf der Entschlüsselung mit S/MIME ... 181
7.11.2 E-Mails mit S/MIME entschlüsseln - Jobbeispiel ... 181
7.11.2.1Allgemeine Einstellungen ... 181
7.11.2.2Adressbedingungen einrichten ... 182
7.11.2.3Crypt Engine/Modus auswählen - Methode ... 183
7.11.2.4Aktionen festlegen ... 186
7.11.2.5Server auswählen / Job Details ... 186
7.12 Signieren mit S/MIME ... 187
7.12.1 Ablauf für S/MIME Signaturen ... 188
7.12.2 E-Mails mit S/MIME signieren - Job einrichten ... 188
7.13 Verifizieren (prüfen) von S/MIME Signaturen ... 189
7.13.1 Ablauf der S/MIME Verifikation ... 189
7.13.2 E-Mail-Signaturen mit S/MIME prüfen - Job einrichten ... 189
8 iQ.Suite Trust ... 191
9 iQ.Suite Trailer ... 193
9.1 Übersicht ... 193
9.1.1 Jobtyp ... 193
9.2 Anhängen von Textbausteinen ... 194
9.2.1 Erstellen eines neuen Textbaustein-Trailers ... 194
9.2.2 Haftungsausschluss anhängen - Jobbeispiel ... 196
9.2.2.1 Allgemeine Einstellungen ... 197
9.2.2.2 Adressbedingungen einrichten ... 198

9.2.2.3 Trailer auswählen ... 198
9.2.2.4 Server auswählen ... 200
9.2.2.5 Details zum Job eingeben ... 201
9.3 Anhängen von individuellen Signaturen ... 202
9.3.1 Erstellen eines neuen Trailers für individuelle Signaturen ... 203
9.3.2 Individuelle Signaturen anhängen - Jobbeispiel ... 205
9.3.2.1 Allgemeine Einstellungen ... 205
9.3.2.2 Adressbedingungen einrichten ... 207
9.3.2.3 Trailer auswählen ... 207
9.3.2.4 Server auswählen ... 209
9.3.2.5 Details zum Job eingeben ... 209
10 iQ.Suite Watchdog ... 211
10.1 Übersicht ... 211
10.1.1 Jobtypen ... 211
10.2 Virenprüfung ... 212
10.2.1 ... ein- und ausgehender E-Mails ... 212
10.2.2 ... im Informationsspeicher ... 214
10.2.3 Virenscanner konfigurieren ... 216
10.2.3.1AntiVir Engine powered by H+BEDV ... 219
10.2.3.2Command Software Scan Engine ... 221
10.2.3.3F-Secure Scan Engine ... 221
10.2.3.4McAfee Scan Engine ... 221
10.2.3.5Norman Scan Engine ... 222
10.2.3.6Sophos Scan Engine (SAVI) ... 223
10.2.3.7Symantec Scan Engine ... 223
10.2.3.8Trend Micro Scan Engine ... 223
10.2.4 Virenprüfung einschalten - Jobbeispiel ... 224
10.2.4.1Allgemeine Einstellungen ... 224
10.2.4.2Adressbedingungen einrichten ... 225
10.2.4.3Virenscanner auswählen ... 226
10.2.4.4Aktionen festlegen ... 228
10.2.4.5Server auswählen ... 233
10.2.4.6Details zum Job eingeben ... 233
10.3 Virenprüfung im Informationsspeicher - Jobbeispiel ... 234
10.3.1 Allgemeine Einstellungen ... 234
10.3.2 Virenscanner auswählen ... 235
10.3.3 Zeitplan festlegen ... 235
10.3.4 Aktionen festlegen ... 236
10.3.5 Job Details ... 239
10.3.6 Server Status ... 239
10.4 Dateieinschränkungen für den Anhang ... 241
10.4.1 ... nach Typ ... 241
10.4.2 ... nach E-Mail-Größe ... 242
10.4.3 ... nach Typ und/oder Anhanggröße ... 243
10.4.4 Fingerprints konfigurieren ... 243
10.4.4.1 Fingerprint mit Namensmuster anlegen ... 245

10.4.4.2 Binärmuster für Fingerprint anlegen 247
10.4.4.3Weitere Fingerprint-Beispiele 251
10.4.5 Dateianhänge nach Typ verbieten - Jobbeispiel 251
10.4.5.1Allgemeine Einstellungen 252
10.4.5.2Adressbedingungen einrichten 253
10.4.5.3Fingerprints auswählen 253
10.4.5.4Aktionen festlegen 255
10.4.5.5Server auswählen / Job Details 256
10.4.6 E-Mail-Größe einschränken - Jobbeispiel 257
10.4.6.1Allgemeine Einstellungen 257
10.4.6.2Adressbedingungen einrichten 258
10.4.6.3E-Mail-Größe festlegen 258
10.4.6.4Aktionen festlegen 259
10.4.6.5Server auswählen / Job Details 260
10.4.7 Anhangtypen und -größe verbieten - Jobbeispiel 260
10.4.7.1Allgemeine Einstellungen 260
10.4.7.2Adressbedingungen einrichten 261
10.4.7.3Fingerprint/Größe bestimmen 262
10.4.7.4Aktionen festlegen 263
10.4.7.5Server auswählen / Job Details 264
11 iQ.Suite Wall 265
11.1 Übersicht 265
11.1.1 Jobtypen 265
11.2 Adressprüfung 266
11.2.1 Absender und/oder Empfänger verbieten - Jobbeispiel 268
11.2.1.1Allgemeine Einstellungen 269
11.2.1.2Adressbedingungen einrichten 270
11.2.1.3Aktionen festlegen 270
11.2.1.4Server auswählen / Job Details 271
11.3 Inhaltsprüfung mit Wortlisten 271
11.3.1 Wortlisten einrichten 272
11.3.1.1Textsuche in Wortlisten 274
11.3.2 Textinhalte prüfen und verbieten - Jobbeispiel 275
11.3.2.1Allgemeine Einstellungen 276
11.3.2.2Adressbedingungen einrichten 277
11.3.2.3Wortlisten auswählen 277
11.3.2.4Aktionen festlegen 280
11.3.2.5Server auswählen / Job Details 281
11.4 Anti-Spam mit dem Wall Spam Filtering Job 281
11.4.1 Definitive Kein-Spam-Kriterien 285
11.4.2 Definitive Spam-Kriterien 286
11.4.3 Praxistipps 287
11.4.4 Anti-Spam-Prüfung - Jobbeispiel 288
11.4.4.1Allgemeine Einstellungen 288
11.4.4.2Adressbedingungen einrichten 289
11.4.4.3Aktionen festlegen 290
11.4.4.4Server auswählen / Job Details 300

11.4.5 Anti-Spam für Experten ... 300
11.4.5.1 Kombinierte Kriterien - Beispiel ... 301
11.4.5.2 Kombination der Hinweise zur Spam-Wahrscheinlichkeit ... 302
11.4.5.3 Kombiniertes Kein Spam-Kriterium ... 303
11.4.5.4 Kombinierte Klassifizierungskriterien ... 304
11.4.5.5 Kombinierte Header-Kriterien ... 305
11.4.5.6 Kombinierte Betreff-Kriterien ... 305
11.4.5.7 Kombinierte Nachrichtentext-Kriterien ... 306
11.4.6 Manuelle Anti-Spam-Konfiguration ... 306
11.5 Anti-Spam mit Wall DCC Spam Filtering ... 307
11.5.1 Was ist DCC? ... 307
11.5.2 Konfiguration der DCC-Einstellungen ... 309
11.5.3 Anti-Spam mit DCC - Jobbeispiel ... 312
11.6 CORE Klassifikation ... 312
11.6.1 Übersicht ... 312
11.6.2 CORE für Anti-Spam verwenden ... 313
11.6.2.1 Standard-Job einschalten ... 313
11.6.2.2 Eigenen Spam-Klassifikator im Standard-Job verwenden ... 313
11.6.3 CORE für Inhaltsklassifizierung verwenden ... 315
11.6.3.1 Neuer CORE Classification Job - Jobbeispiel ... 317
11.6.3.2 Job duplizieren ... 322
11.6.3.3 Einstellungen für alle anderen Kategorien wiederholen ... 322
11.7 Limitieren der Anzahl der Empfänger ... 322
11.7.1 Empfängeranzahl begrenzen - Jobbeispiel ... 322
11.7.1.1 Allgemeine Einstellungen ... 322
11.7.1.2 Adressbedingungen einrichten ... 323
11.7.1.3 Anzahl Empfänger festlegen ... 324
11.7.1.4 Aktionen festlegen ... 324
11.7.1.5 Server auswählen / Job Details ... 325
12 iQ.Suite Bridge ... 327
13 Glossar ... 329
Index ... 353

1 Vorwort

1.1 Qualitätssicherung

Herzlichen Dank, dass Sie sich für die iQ.Suite von GROUP Technologies entschieden haben. Mit dieser Software erhalten Sie die führende Lösung für E-Mail Lifecycle Management.

Die iQ.Suite ist ein hochwertiges Produkt, das Sie bei allen Aufgaben rund um das Management von E-Mail unterstützt. Mit diesem modularen Programmpaket sichern Sie Ihre Software-Infrastruktur vor Viren, Spam und unlauteren Inhalten sowie vor dem Verlust vertraulicher Informationen. Profitieren Sie außerdem von der Verschlüsselung, Klassifizierung und sicheren Archivierung von E-Mails in Ihrem Unternehmen.

Unsere Produkte stehen für Innovation und Qualität zur Zufriedenheit unserer Kunden. Sie werden intensiven Abschlusstests unterzogen. Kein Produkt verlässt unser Haus ohne einen ausgiebigen Test durch unser QA-Team.

Die iQ.Suite für Exchange ist

Auf eine erfolgreiche Zusammenarbeit.

Ihr GROUP Technologies Team

1.2 Hotline

Sollten Sie Fragen oder Probleme haben, können Sie sich jederzeit an uns wenden. Sie erreichen uns von 8:30 bis 18:00 Uhr

- Europa, Asien, andere
  - Tel.: +49 721 49 01 112

- Fax: +49 721 49 01 1912
- E-Mail D: hotline@group-technologies.com

- USA & Canada:
  - Tel.: 877 476 8755 (gebührenfrei)
  - Tel.: +1 508 473 3332
  - Fax: +1 508 473 9940
  - E-Mail: hotline@group-software.com
  - Unsere aktuellen FAQs finden Sie auf unserer Webseite: www.group-technologies.com

1.3 Ein Fehler: Was nun?

Um im Fall eines Fehlers eine optimale Hilfestellung gewährleisten zu können, benötigen wir folgende Informationen:

- Produktversion
- Ihre Lizenznummer
- Exchange-Server-Version inkl. Service Pack
- Betriebssystem und -version inkl. Service Pack
- Konfigurationsdateien
- Protokolldateien

1.4 Urheberrecht

GROUP Technologies AG, nachfolgend GROUP genannt, ist Inhaber sämtlicher gewerblicher Schutz- und Urheberrechte dieser Dokumentation. GROUP behält sich alle Rechte vor, die nicht ausdrücklich gewährt wurden.

Copyright 1992-2005 GROUP Technologies AG,
Alle Rechte vorbehalten.

1.5 Gewährleistung

GROUP übernimmt keine ausdrückliche oder stillschweigende Gewähr für die Dokumentation. Dies umfasst auch Qualität, Ausführung, Handelsüblichkeit oder Eignung für einen bestimmten Zweck.

Die Produktbeschreibungen haben lediglich allgemeinen und beschreibenden Charakter. Sie verstehen sich weder als Zusicherung bestimmter Eigenschaften noch als Gewährleistungs- oder Garantieerklärung. Spezifikationen und Design

unserer Produkte können ohne vorherige Bekanntgabe jederzeit geändert werden, insbesondere, um dem technischen Fortschritt Rechnung zu tragen. Bitte wenden Sie sich für die jeweils aktuellsten Informationen an unseren Vertrieb.

1.6 Lizenzvereinbarungen

Die Lizenzvereinbarungen von GROUP stehen auf der GROUP Webseite und auf der Produkt-CD zur Verfügung. Lizenzvereinbarungen anderer beteiligter Softwarehersteller sind als PDF dem Softwareprodukt beigefügt.

1.7 Copyright Vermerke Dritter

iQ.Suite for Exchange includes the following software:

Anti Vir Engine powered by H+BEDV

Copyright (c) 2004 H+BEDV Datentechnik GmbH

iQ.Suite for Exchange includes ZLib software:

ZLib 1.1.4 (c) 1995-2002 Jean-loup Gailly and Mark Adler.

iQ.Suite for Exchange includes software developed by the Apache Software Foundation (http://www.apache.org/):

Xerxes 2.1.0 (c) 1999-2001 The Apache Software Foundation.

All rights reserved.

iQ.Suite for Exchange includes software developed by Robert A. van Engelen:

gSOAP (c) 2001-2002 Robert A. van Engelen, Florida State University.

All Rights Reserved.

iQ.Suite for Exchange includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/):

Open SSL (c) 1998-2002 The OpenSSL Project. All rights reserved.

iQ.Suite for Exchange includes cryptographic software written by Eric Young (eay@cryptsoft.com):

Original SSLeay (c) 1995-1998 Eric Young. All rights reserved.

iQ.Suite for Exchange includes the following software:

The Expat XML Parser

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

and Clark Cooper
Copyright (c) 2001, 2002 Expat maintainers. All rights reserved.

iQ.Suite for Exchange includes the **STL Port DLL**
Copyright 1999,2000 Boris Fomitchev

iQ.Suite for Exchange includes the file **dbghelp.dll**,
Copyright (c) Microsoft Corporation

Microsoft, Windows und das Windows Logo sind eingetragene Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern.

Alle weiteren Informationen über eingebundene Drittprodukte entnehmen Sie bitte dem „Third Party License Agreements“ Dokument, welches im `..GROUP Technologies\iQ.Suite\Data`-Verzeichnis zur Verfügung steht.

2 Einleitung

2.1 Der Sinn eines Handbuchs

Sie möchten mit Ihrer neuen Anwendung virtuos umgehen können. Wir möchten Ihnen dabei helfen. Wir haben deshalb versucht, uns in diesem Handbuch so allgemein verständlich wie nur möglich auszudrücken. Sollten Sie Anregungen für Verbesserungen haben, sind wir für eine Rückmeldung dankbar. Schreiben Sie uns eine E-Mail:
manual@group-technologies.com

2.2 Aufbau dieses Handbuchs

Wir halten uns in diesem Buch weitgehend an folgende Richtlinien:

fett	Menünamen und -einträge, Namen von Fenstern, Eingabe- und Listenfeldern, Meldungen, Dateinamen sowie wichtige Aussagen sind **fett** gedruckt.
kursiv	Eingaben, die Sie als Administrator vornehmen müssen, sind *kursiv* geschrieben.
`Festbreite`	Programmcode und Pfade stehen in `Festbreitenschrift`.
Links	Bei unterstrichenem Text handelt es sich um einen Hyperlink, den wir normalerweise blau eingefärbt haben.

Wir verwenden folgende Symbole:

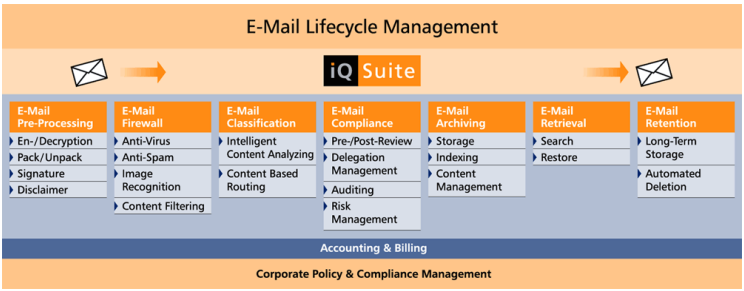
Das Infosymbol steht für einen Hinweis. Es weist Sie auf Besonderheiten hin, die Sie beachten müssen, damit Sie problemlos mit Ihrem System arbeiten können.

Das Auge heißt Achtung. Sehen Sie genau hin! Hier kommen wichtige Passagen im Text, welche Sie beachten sollten, wenn Sie nicht evtl. Datenverlust, Beschädigung Ihres Systems oder andere unangenehme Begleiterscheinungen riskieren wollen. Lesen Sie diese Passagen besonders aufmerksam.

Kleine Geschenke erhalten die Freundschaft! Neben diesem Päckchen geben wir Ihnen Hilfestellungen zu einem bestimmten Problem, verraten Tipps und Tricks oder ungewöhnliche Lösungen und Besonderheiten.

Technische Erläuterungen zu vielen Begriffe finden Sie im “Glossar” auf Seite 329.

3 E-Mail Lifecycle Management - Produktüberblick



Unter E-Mail Lifecycle Management versteht man Strategien und Methoden, um E-Mails von der Entstehung bis zur Entsorgung in Übereinstimmung mit den unternehmensspezifischen Geschäftsprozessen und gesetzlichen Vorschriften zu verarbeiten, abzuspeichern und zu verwalten. E-Mail Lifecycle Management gewährleistet effektive Geschäftsprozesse in jedem Unternehmen. Die iQ.Suite von GROUP Technologies AG ist das führende Programmpaket zur Realisierung von E-Mail Lifecycle Management und die ideale Lösung zur Umsetzung sicherer und effizienter Geschäftsprozesse. Mit der iQ.Suite durchlaufen E-Mails alle Prozesse auf einer einzigen Plattform, von der Verschlüsselung und Virenschutz über Anti-Spam und Content Filtering bis hin zur Klassifizierung und langfristigen Archivierung.
Über den gesamten Lebenszyklus lassen sich alle E-Mails regelbasiert steuern und automatisiert verarbeiten. Archivsysteme von Drittherstellern können nahtlos an die iQ.Suite angebunden und für die revisionssichere E-Mail-Archivierung genutzt werden.

Die Produkte sind beliebig kombinier- und skalierbar. Je nach Anforderung kommen die gewünschten Module zum Einsatz. Weitere Produkte lassen sich einfach hinzufügen. Die einzelnen Produkte nutzen gemeinsam ein regelbasiertes Sicherheitskonzept. Die direkte Interaktion aller Funktionen gewährleistet optimale Leistung und Sicherheit. Konfigurierbare Benachrichtigungen an Absender, Empfänger und Administrator liefern Transparenz. Alle Produkte werden einheitlich zentral verwaltet. Gemeinsame Protokolle, Statistiken und Fehlerreports verringern die Kosten für die Administration erheblich.

3.1 E-Mail Pre-Processing

Aufbereitung von E-Mails für die Weiterverarbeitung bzw. den Versand.

Gepackte Dateien entpuppen sich häufig als Virenfallen, insbesondere wenn sie verschlüsselte Viren enthalten. Diese werden oft unerkannt an Virenscannern vorbeigeschleust. E-Mail Pre-Processing sorgt dafür, dass eingehende E-Mails zuerst serverseitig entschlüsselt und entpackt werden. Die anschließende Spam- und Virenprüfung identifiziert die Eindringlinge und stellt sie in Quarantäne. Geprüfte E-Mails können dann wieder automatisiert verschlüsselt und weitergeleitet werden. Ausgehende E-Mails lassen sich signieren, mit Legal Disclaimer versehen, packen, automatisiert verschlüsseln und versenden. E-Mails werden zentral, vollautomatisch und adressenbasiert auf dem Mail-Server verschlüsselt. Dabei kommen PGP, GnuPG oder S/MIME zum Einsatz, die auch parallel betrieben werden können. Die Schlüssel lassen sich ohne aufwändige Public-Key-Infrastructure (PKI) serverseitig verwalten und digitale Zertifikate komfortabel erstellen und pflegen.

3.1.1 iQ.Suite Crypt

Datensicherheit, Datenintegrität, gesetzliche Vorschriften zum Datenschutz und der Schutz vor Wirtschaftsspionage verlangen die Verschlüsselung des elektronischen Briefverkehrs bei der Nutzung des Internets. iQ.Suite Crypt ermöglicht durch flexible Konfigurationen die Festlegung unternehmensweiter Verschlüsselungsrichtlinien an zentraler Stelle. E-Mails werden mit starken asymmetrischen und symmetrischen Verfahren verschlüsselt. iQ.Suite Crypt verwendet hierbei Standardverfahren wie PGP oder S/MIME, die auch parallel einsetzbar sind. Die Verwendung für die Benutzer ist vollständig transparent.

- Serverbasierte, zentrale Verschlüsselung von E-Mails, dadurch transparente E-Mail-Verschlüsselung unabhängig vom E-Mail-Client für den Benutzer und keine Schlüsselverwaltung/Schulungsaufwand beim Endbenutzer.
- Vergabe zentraler Verschlüsselungsrichtlinien für die Kommunikation über Internet und öffentliche Netze.
- Gezieltes Verschlüsseln durch Adressprüfung beliebiger Absender-Empfänger-Kombinationen, Empfängergruppen und Internetdomänen.
- Automatischer Import von neuen Schlüsseln.

- Integrierbar in jede Schlüsselverwaltung und Public Key Infrastructure (PKI).
- Separate Zertifikatsverwaltung für S/MIME in eigener Zertifikatsdatenbank.
- Zentrale Ablage von personen- und firmenbezogenen Public Keys auf dem Server.
- Verwendung vorhandener LDAP-Verzeichnisse.
- Parallele Unterstützung von PGP, GnuPG und S/MIME.
- Gleichzeitige Verwendung unterschiedlicher Verfahren mit langen Schlüsseln, z.B. PGP, S/MIME.
- Server-zu-Server Verschlüsselung zum Aufbau sicherer Kommunikationskanäle.
- Client-zu-Server Verschlüsselung, z. B. für externe Endbenutzer mit clientbasierter Verschlüsselung anderer Dritthersteller.
- Voll kompatibel zu Ende-zu-Ende Verschlüsselung.

3.1.2 iQ.Suite Trust

iQ.Suite Trust ist die Grundlage, um die Aufgaben eines Trustcenters zur Erstellung von Zertifikaten zu übernehmen.

- Erstellung von X.509-Zertifikaten gemäß eigener Unternehmensrichtlinien.
- Überwachung der Gültigkeit von X.509-Zertifikaten.
- Erstellung separater öffentlicher und privater Schlüssel.
- Offline Administrationswerkzeug unabhängig von der Mailplattform.
- RSA-Unterstützung bis 4.096 Bit
- ECC-Unterstützung bis 256 Bit.
- Unterstützt den Einsatz von Smartcard-Geräten.
- Effektiver Einsatz zusammen mit Crypt.

3.1.3 iQ.Suite Trailer

Rechtssicherheit ist aufgrund des immer größer werdenden Mailaufkommens in Firmen ein wichtiges Thema. iQ.Suite Trailer nutzt E-Mail-Kopf- und -Fußzeilen zur Integration von Textbausteinen. Rechtshinweise, ein Haftungsausschluss, Sicherheitshinweise, Verzichtserklärungen und Unternehmensinformationen können in ausgehende E-Mails eingebunden werden. Mit zusätzlichen Funktionen ist

es möglich, die zeitliche Verwendung der Texte abhängig von Personen, Gruppen und Internetdomänen einzuschränken.

- Rechtliche Absicherung durch einen einheitlichen Haftungsausschluss
- Individuelle Textbausteine für verschiedene Benutzergruppen und Empfänger.
- Integration von dynamischen Benutzerinformationen aus dem zentralen E-Mail-Adressbuch.
- Absender-/Empfänger-abhängige Integration von Textanhängen, z. B. abteilungsspezifisch.
- Individuelle Textanhänge nach frei definierbaren Zeiträumen.
- Mehrsprachige Textanhänge für unterschiedliche Empfänger.
- Erstellung, Aktivierung und Pflege durch Verantwortliche in den Fachbereichen.
- Umsetzung fertig gestalteter Textsignaturen, die dem Corporate Design entsprechen.
- Unterstützung multipler Formate (HTML, Text).
- Wahl der Position von Textbausteinen innerhalb der E-Mail (Top/Bottom).
- Verkettung mehrerer Textbausteine pro E-Mail.
- Konfigurierbare Regeln für alle Funktionen

3.2 E-Mail Firewall

Schutz vor gefährlichen und unerwünschten E-Mails bzw. vor Verlust vertraulicher Informationen.

Die Versendung von Dateien auf dem Mailweg über das Internet und die Replikation von Datenbanken lassen Viren leicht in Netzwerke eindringen, wenn nicht schon auf dem Server Abwehrmaßnahmen ergriffen werden. Fast täglich berichten die Medien von neuen Viren und steigendem Spam-Aufkommen. Ein wirkungsvoller Schutz gegen Risiken und Gefahren ist unerlässlich. Mit der iQ.Suite lassen sich eingehende E-Mails regelbasiert nach Viren, Spam, unerwünschten Bildern, Dateien und Textinhalten filtern. Integrierte Virenscanner überprüfen die gesamte E-Mail auf bösartigen Code. Kritische Dateitypen werden anhand eindeutiger Dateimuster-Informationen, den so genannten Fingerprints, gefiltert. Beliebige Virenscanner führender Hersteller lassen sich parallel betreiben. Vor der Zustellung überprüft die iQ.Suite E-Mails gemäß den Unternehmensrichtli-

nien rundum auf Spam: Adressdaten, Betreffzeile, E-Mail-Text, Dateianhänge und Bilddateien. Bei ausgehenden E-Mails lässt sich der Versand sensibler Informationen unterbinden. Die integrierte CORE-Technologie (Content Recognition Engine) klassifiziert und filtert E-Mails automatisch entsprechend individueller Anforderungen. CORE garantiert Ihnen höchste Erkennungsraten bei Anti-Spam und keine „False Positives“ (fälschlicherweise als Spam deklarierte E-Mails).

3.2.1 iQ.Suite Watchdog

iQ.Suite Watchdog schützt Ihre Microsoft Exchange-Umgebung umfassend vor E-Mail-Attacken, E-Mail-Viren und bedrohlichen Inhalten. iQ.Suite Watchdog entfernt alle Viren sowie andere kritische Dateianhänge zuverlässig und stellt sie in sichere Quarantäne. Es werden alle E-Mails und Datenbanken auf dem Server kontrolliert.

- Rekursive Virenprüfung aller E-Mails und Dateianhänge in Echtzeit, ereignis- und zeitgesteuert.
- Informationsspeicher-Scan auf jedem Server
- Keine Beeinträchtigung der Replikationszeit durch die Prüfung.
- Leistungsstarker Virenscanner bereits integriert.
- Unterstützung automatischer Virenpattern-Updates.
- Paralleler Einsatz mehrerer Virenscanner unterschiedlicher führender Dritthersteller.
- Scannen von E-Mail-Nachrichtentext und Anhängen.
- Erkennung von Dateianhängen mittels eindeutiger, nicht manipulierbarer Dateimuster („Fingerprints“) oder anhand des Dateityps, erkennt und blockt auch manipulierte Dateien.
- Definition von Dateieinschränkungen durch Kombination von Dateiname, Dateierweiterung und Dateigröße.
- Anwendung der Dateieinschränkungen auf Archive, z. B. zip, rar.
- Erstellung und Einsatz eigener Dateimuster zur Sicherstellung des Austausches aktueller Informationen (z. B. Preislisten, AGBs).
- Automatische Erkennung von neuen Postfächern
- Prüfung verschlüsselter E-Mails auf Viren in Kombination mit Crypt

3.2.2 iQ.Suite Wall

Die gesetzlichen Vorschriften zum Schutz vor sexuellen und rassistischen Belästigungen, zunehmende elektronische Werbung und neueste Angriffsmethoden durch Hacker zwingen zur Abwehr. iQ.Suite Wall bietet Schutz vor Missbrauch und unkontrollierter Nutzung von E-Mail und Datenbanken. Das Produkt sichert umfassend vor Belästigungen durch Spam- und Junk-Mails und der Gefahr durch das Versenden vertraulicher Informationen.

- Analyse des gesamten Inhaltes einer E-Mail inklusive der Anhänge (Betreff, Nachrichtentext, Dateianhänge) mittels Lexikon und des intelligenten, lernfähigen CORE
- Prüfung gemäß der Unternehmensrichtlinien auf verbotene, nicht erwünschte oder vertrauliche Inhalte.
- Blocken von E-Mails unerwünschter Absender (Spam-Versender, Mailinglisten etc.) sowie an unerwünschte Empfänger (z. B. Mitbewerber).
- Verwendung aktueller Spam-Pattern für die schnelle Erkennung neuer Spammer-Tricks.
- Verwaltung von White- und Blacklists am Server für effektives Blocken ausschließlich unerwünschter E-Mails.
- Festlegung von Sender-/Empfänger-Kanälen zur Regelung einer dedizierten E-Mail-Kommunikation.
- Frei editierbare Ausschlusslisten für Adressen und Inhalte in Betreff und Nachrichtentext
- Zentrale Prüfung verschlüsselter E-Mails durch die Kombination von Wall und Crypt, anstelle von clientbasierter Ende-zu-Ende-Verschlüsselung, welche die zentralen E-Mail-Sicherheitsprüfungen unterwandert.
- Flexible Benachrichtigungen über geblockte E-Mails (direkt oder zeitgesteuert) an Administration oder E-Mail-Empfänger / -Absender.
- Benutzerspezifischer Zugriff auf E-Mails in der Quarantäne.
- Zentrales Quarantäne-Management besonders effizient bei Enterprise- / Mehr-Server-Umgebungen.

3.3 E-Mail Classification

Erkennung und Klassifizierung von Inhalten bzw. inhaltsbasierte Weiterverarbeitung von E-Mails.

Das Regelwerk ist ein durchgängiges Funktionsmerkmal der iQ.Suite. Es erlaubt Unternehmen, gemäß eigener Richtlinien individuelle Geschäftsprozesse sicherzustellen. E-Mails lassen sich so nach voreingestellten Inhalten oder Adressaten automatisch kategorisieren, weiterleiten oder weiterverarbeiten. Die Umsetzung übernimmt die in die iQ.Suite integrierte CORE-Technologie (Content Recognition Engine), ein statistisches Verfahren zur Überprüfung und Autoklassifizierung von E-Mails. CORE erkennt als selbst lernender Filter auch komplexe Inhalte nach individuellen Kriterien. Eingehende E-Mails lassen sich aufgrund der Klassifizierung auf Wunsch an den passenden Empfänger weiterleiten. So gelangt zum Beispiel eine unpersönlich adressierte Support-Anfrage direkt an den Mitarbeiter, der für das angesprochene Problem am besten geeignet erscheint. Über dieses adressen- und inhaltsbasierte Routing ist sichergestellt, dass geschäftsrelevante Nachrichten in den richtigen Postfächern ankommen und automatisch Maßnahmen zur Weiterverarbeitung eingeleitet werden.

3.3.1 iQ.Suite Wall

Die automatische Organisation und kontextbasierte Ablage von Inhalten, der Aufbau flexibler Zustell- und Verteilungsmechanismen sowie die automatisierte Indexierung für die E-Mail-Archivierung sind Beispiele für die inhaltsabhängige Weiterverarbeitung, die durch Klassifizierung und Kategorisierung ebenfalls mit iQ.Suite Wall realisiert werden können.

- Bildung unternehmensspezifischer E-Mail-Kategorien.
- Optimierung von Klassen durch das CORE-Teaching bei Verwendung geringer Lernmengen.
- Automatische Zuordnung von E-Mails zu einer oder mehreren Kategorie/n (Multiklassifikation).
- Verwendung der Content Recognition Engine: einem statistischen Verfahren unter Verwendung von Support Vector Machines (SVM) zur Überprüfung und Autoklassifizierung von E-Mails.

- Response-Management durch definierte Klassifizierungen beispielsweise für den Kundensupport: automatische Weiterleitung der E-Mails an qualifizierte Mitarbeiter.
- Dokumentenschutz: Nach entsprechenden Kategorien können beispielsweise alle ausgehenden E-Mails auf firmenrelevante Inhalte geprüft werden. Eine Inhaltsprüfung von E-Mail-Anhängen ist ebenfalls möglich.

3.4 E-Mail Compliance

Übereinstimmung mit und Erfüllung von rechtlichen und regulativen Vorgaben.

Mit der iQ.Suite sind Unternehmen in der Lage, E-Mails gesetzeskonform und gemäß unternehmensinterner Vorschriften zu senden und zu empfangen. Basierend auf den individuellen Regelwerken von Unternehmen lassen sich E-Mails automatisch anhalten und nach dem Vier-Augen-Prinzip prüfen. Erst nach Freigabe werden sie versendet, in Quarantäne gestellt, an Dritte weiter geleitet oder gelöscht. Durch diesen Prüfprozess erreichen ausschließlich unternehmenskonforme E-Mails den Empfänger. Ausgehende E-Mails können nicht für den unautorisierten Versand sensibler Dokumente missbraucht werden. Für interne oder externe Audits ist gewährleistet, dass sich die E-Mail-Korrespondenz lückenlos nachvoll ziehen und wiederherstellen lässt. Das regelbasierte und einheitliche Vertretungsmanagement stellt sicher, dass bei Abwesenheit des E-Mail-Empfängers alle wichtigen Nachrichten von autorisierten Vertretern zu bearbeiten sind. Gleichzeitig ist sichergestellt, dass vertrauliche Nachrichten nicht weitergeleitet werden.

3.4.1 iQ.Suite Bridge

Die Ausrichtung von unternehmensinternen Abläufen im Zusammenhang mit E-Mail ist immer häufiger an die Einhaltung von Gesetzen, Verordnungen (Regulatory Compliance wie SOX, HIPAA, GDPdU, etc.) sowie Unternehmensrichtlinien (Corporate Compliance) gebunden. Mit iQ.Suite Bridge realisieren Sie die nahtlose Anbindung an ein Compliance-System.

- Proaktive Pre-Review – E-Mails können vor der Zustellung zur Überprüfung an ein Compliance-System übergeben werden.

- Post-Review – E-Mails können nach Zustellung stichprobenartig oder vollständig auf Gesetzeskonformität überprüft werden.
- Re-Routing von fälschlich adressierten E-Mails nach Compliance-Vorgaben.
- Sicherstellung der lückenlosen E-Mail-Kommunikation für Audits durch Post-Review Funktionen.
- Workflow-Prinzip: Sendung bzw. Weiterleitung von E-Mails erst nach Freigabe durch autorisiertes Personal entsprechend Compliance-Anforderungen.
- DXL/XML-Export ins Dateisystem für flexibel definierbare Weiterverarbeitung.
- Automatische Überwachung von verfügbarem Speicherplatz auf dem Server.
- Anbindung von Archivsystemen zur Erweiterung um Archivierungsfunktionen.

3.5 E-Mail Archiving, Retrieval, Retention

Ablage und Verwaltung, Suche, Wiederherstellung und Löschen von E-Mails.

Unternehmen sind verpflichtet, E-Mails über festgelegte Zeiträume aufzubewahren. Hierfür lässt sich das integrierte iQ.Suite Archivierungsmodul einsetzen sowie führende Archivierungslösungen von Drittherstellern nahtlos anbinden. Die Archivierung ist der Zustellung vorgeschaltet, um Manipulationen durch Anwender auszuschließen. iQ.Suite übergibt wichtige Metadaten wie E-Mail-Header, Verarbeitungsdetails oder Kategorie, für die Indexerstellung automatisch an das Archivsystem. Die E-Mail-Korrespondenz ist anhand von Schlagwörtern zu einem späteren Zeitpunkt, etwa für eine Steuerprüfung, wiederherstellbar. Die gesetzlich geforderte Revisionssicherheit ist gewährleistet.

3.5.1 iQ.Suite Bridge

Mit dem Schnittstellen- und Integrationsmodul iQ.Suite Bridge ist es erstmals möglich, eine E-Mail-Archivierung auf der Grundlage fein abstimmbarer Richtlinien zur Vorverarbeitung, Filterung und Klassifizierung von E-Mails aufzubauen. Sie integrieren eine flexible Gesamtlösung, welche die vielfältigen Auflagen bis

ins Detail erfüllt und die nahtlose Integration von E-Mail in die Geschäftsprozesse sicherstellt.

- Anbindung führender Archivsysteme an das E-Mail-System.
- Wiederherstellung archivierter E-Mails mittels komfortabler, interaktiver Importfunktion.
- Lückenlose Archivierung von E-Mails vor der Zustellung durch proaktiven oder zeitgesteuerten Export.
- Austausch von speicherintensiven E-Mail-Inhalten durch Links auf die archivierten Daten.
- Flexibles Metadaten-Set und mögliche Vorklassifikation von E-Mails.
- Klassische Funktionen von Archivsystemen können genutzt werden: gesetzeskonforme, revisionssichere Archivierung von Daten, Indizierung (Metadaten), Suchen, Wiederauffinden und Wiederherstellen der Daten im Archiv.
- Automatische Überwachung von verfügbarem Speicherplatz auf dem Server.

3.6 Leistungsmerkmale aller Produkte

- Umfassende Filter
- Reporting und Statistik
- Quarantäne-Management, auch benutzerspezifisch
- Zentrale, integrierte Administration über Microsoft Management Konsole
- Vollständige Integration in Exchange 2000/2003 und optional in Windows 2000/2003 Active Directory
- Detaillierte Protokollfunktionen
- Skalierbare Architektur
- “Ready to go" für Application Service Providing (ASP)
- Optimales Zusammenspiel und einfache Erweiterung mit weiteren iQ.Suite Produkten

4 Quickstart

4.1 Installation auf einem Exchange-Server

Aktivieren Sie mit einem Doppelklick die Datei

setup_iqsuite_msx_de.exe

im Installationspaket.

Befolgen Sie die weiteren Anweisungen des InstallShield Wizard, bis die Installation abgeschlossen ist. Das Standardverzeichnis für die Installation der iQ.Suite ist - falls Sie nichts anderes angeben:

`C:\Programme\GROUP Technologies\iQ.Suite\` (deutsch)

`C:\Program Files\GROUP Technologies\iQ.Suite\` (englisch).

Deaktivieren Sie in jedem Fall eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virenscanner für das Verzeichnis `..\iQ.Suite\GrpData`!

Nähere Informationen zur Installation finden Sie in "Installation" auf Seite 25.

4.2 Installation auf mehreren Exchange-Servern

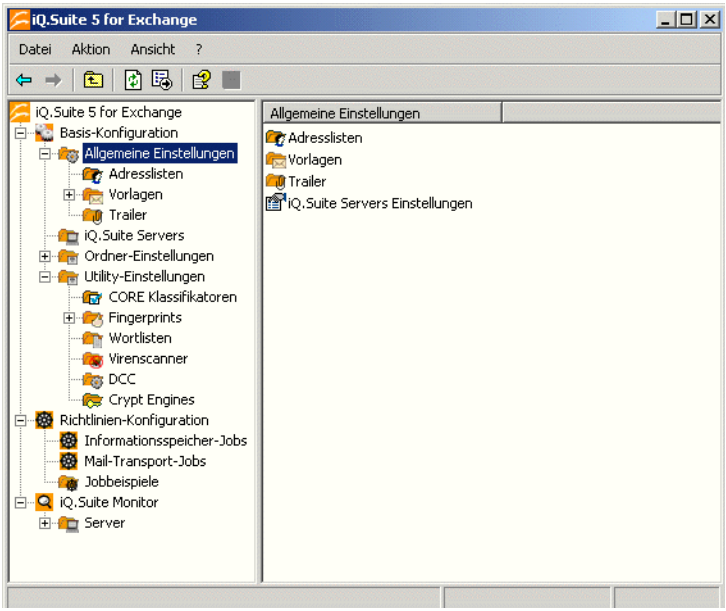
Bitte lesen Sie dazu unbedingt das Kapitel "Installation der iQ.Suite auf mehreren Exchange-Servern" auf Seite 31.

4.3 Starten der iQ.Suite Konsole

Die iQ.Suite ist ein Serverprodukt, das durch die iQ.Suite Konsole konfiguriert wird. Damit die iQ.Suite arbeitet, muss der iQ.Suite Service gestartet sein. Näheres über den iQ.Suite Service finden Sie unter "Der iQ.Suite Service = Enterprise Message Handler (EMH)" auf Seite 73. Sie starten die Konsole über

--> Programme --> GROUP Technologies --> iQ.Suite --> iQ.Suite Konsole. Bevor Sie die iQ.Suite Konsole schließen können, werden Sie gefragt, ob Sie eventuelle Änderungen speichern wollen.

Offene Änderungen werden durch **(*)** am obersten Knoten angezeigt. Wenn Sie Ihre Konfiguration zwischenspeichern wollen, können Sie das innerhalb der iQ.Suite mit der Schaltfläche tun. Die Konfiguration wird in der Datei **ConfigData.xml** gespeichert, die im Verzeichnis `GROUP Technologies\iQ.Suite\Config` abgelegt ist.



4.4 Konfiguration in der iQ.Suite Konsole

Die Konfiguration teilt sich in zwei Bereiche:

1. **Basis-Konfiguration**

   Einstellen der gültigen Server, E-Mail-Adressen, gemeinsamen Vorlagen und Utility-Einstellungen.

2. **Richtlinien-Konfiguration**

   Einstellen und aktivieren aller gewünschten Jobs nach Firmenrichtlinien.

Im **iQ.Suite Monitor** können Sie die **Quarantänen** und **CORE Klassifikatoren** der konfigurierten Server einsehen und administrieren, umfangreiche Filtermöglichkeiten anwenden und die E-Mails erneut versenden.

4.4.1 Basis-Konfiguration

1. Konfigurieren Sie unter **Allgemeine Einstellungen --> iQ.Suite Servers-Einstellungen** die interne Domäne und die Benachrichtigungs-E-Mail-Adressen.
2. Konfigurieren Sie die **Adresslisten** (für die Auswahl in den Job-Regeln) und **Trailer** (für iQ.Suite Trailer) unter **Allgemeine Einstellungen**.
3. Ändern Sie ggf. die Standard-**Vorlagen** unter **Allgemeine Einstellungen**.

4. Konfigurieren Sie unter Utility-Einstellungen das benötigte Zubehör wie **CORE Klassifikatoren, Wortlisten** und den/die **DCC**-Server (für iQ.Suite Wall), **Fingerprints** und **Virenscanner** (für iQ.Suite Watchdog) und die **Crypt Engines** (für iQ.Suite Crypt).

Weitere Informationen zur Basis-Konfiguration finden Sie in "Basis-Konfiguration" auf Seite 85. Die modulspezifischen Einstellmöglichkeiten sind in den entsprechenden Kapiteln "iQ.Suite Crypt" auf Seite 135, "iQ.Suite Trailer" auf Seite 193, "iQ.Suite Watchdog" auf Seite 211, "iQ.Suite Wall" auf Seite 265 und beschrieben. Informationen zu weiteren Anpassungsmöglichkeiten finden Sie in "Konfiguration in der iQ.Suite Management Konsole" auf Seite 84.

4.4.2 Richtlinien-Konfiguration

1. Suchen Sie sich unter **Jobbeispiele** den gewünschten Job aus.
2. Um einen Job neu anzulegen, markieren Sie den Job und ziehen Sie ihn in den Ordner **Mail-Transport-Jobs**. Konfigurieren Sie den Namen und die Eigenschaften dieses Jobs und schalten Sie den Job unter **Eigenschaften** aktiv.
3. Achten Sie auf die Reihenfolge der Abarbeitung der Jobs (siehe "Prioritäten der Jobs" auf Seite 122).
4. Speichern Sie Ihre Änderungen, siehe auch "Starten der iQ.Suite Konsole" auf Seite 17.

Informationsspeicher-Jobs können nicht selbst angelegt werden. Sobald Sie einen neuen Server angegeben haben, steht automatisch ein Informationsspeicher-Job zur Verfügung. Wenn Sie den Server wieder entfernen, wird auch der Informationsspeicher-Job gelöscht.

Nähere Informationen über die Einrichtung von Jobs und Unternehmensrichtlinien finden Sie in "Richtlinien-Konfiguration" auf Seite 118.

4.4.3 iQ.Suite Monitor

Im iQ.Suite Monitor beobachten Sie die aktuellen „Live-Daten" und administrieren beispielsweise **Quarantänen**.

1. Klicken Sie auf den gewünschten Server.
2. Authentifizieren Sie sich mit einem Benutzernamen und Passwort, der auf dem Dateisystem des Servers Berechtigungen für die iQ.Suite Daten

besitzt. Näheres zur Anmeldung finden Sie in "iQ.Suite Monitor" auf Seite 123.

3. Klicken Sie in den Bereich, den Sie einsehen wollen, also auf **Standard-Quarantäne** (falls Sie keine weiteren angelegt haben) oder **Badmail**. Alle vorhandenen Mails werden angezeigt (Anzeigegrenze 10.000 Mails).
4. Filtern Sie die gewünschten Mails mit dem Filteroptionen-Icon aus.
5. Öffnen Sie eine Mail mit einem Doppelklick.
6. Versenden Sie die Mail mit bei Bedarf erneut.

Nähere Informationen finden Sie ab Kapitel "iQ.Suite Monitor" auf Seite 123.

4.5 Notwendige Schritte nach der Installation

1. **iQ.Suite Servers** konfigurieren
2. Wenn Sie iQ.Suite Watchdog verwenden: **Virenscanner** aktiv schalten
3. iQ.Suite Jobs auswählen und aktiv schalten

4.5.1 Einstellungen von iQ.Suite Servers

iQ.Suite Servers-Einstellungen bezeichnet **alle** Server, auf denen die iQ.Suite installiert ist. Für diese Server können Sie übergreifende Einstellungen vornehmen, die für **alle** Server gültig sind. Jeder Server kann zusätzlich individuell konfiguriert werden: Näheres unter "Einstellungen für einen einzelnen iQ.Suite Server" auf Seite 85.

Wählen Sie **Basis-Konfiguration --> Allgemeine Einstellungen**, klicken Sie im **rechten** Fensterbereich auf **iQ.Suite Server-Einstellungen** und wählen Sie mit der rechten Maustaste **Eigenschaften** oder öffnen Sie die Eigenschaften per Doppelklick. Alternativ können Sie im linken Fensterbereich unter **Basis-Konfiguration** mit einem rechten Mausklick auf **iQ.Suite Servers** die **Eigenschaften** aufrufen.

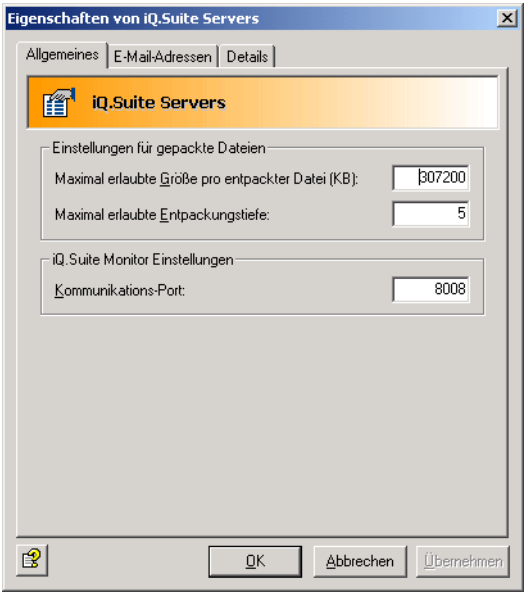
4.5.1.1 Gepackte Dateien und iQ.Suite Monitor

Die Einstellungen auf der Registerkarte **Allgemeines** legen die maximal erlaubte Größe entpackter Dateien auf der Festplatte[1] und die maximal erlaubte Entpa-

1. siehe dazu auch ZIP of Death im "Glossar" auf Seite 329

ckungstiefe bei Archiven[2] fest. E-Mails, die diese Werte überschreiten, werden in den Bad-Mail-Bereich überführt.

Achten Sie auf die korrekte Einstellung Ihres Kommunikationsports für den **iQ.Suite Monitor**[3]. Die Kommunikation mit den Servern ist sonst nicht möglich. Üblicherweise wird *8008* verwendet, der als Standardport bei der Installation eingetragen wird. Die hier eingetragenen Werte gelten für **alle** Server.



Lesen Sie in diesem Zusammenhang auch die Beschreibung zur Rechtevergabe und Sicherheitseinstellungen unter "iQ.Suite Monitor" auf Seite 123.

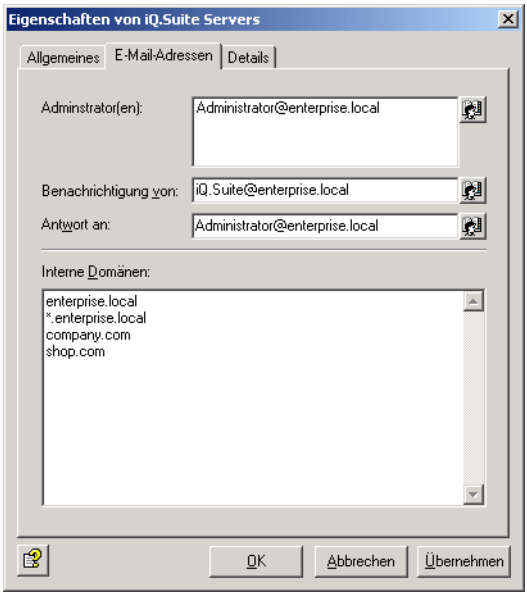
4.5.1.2 Definition der E-Mail-Adressen und internen Domänen

Während der Installation wird automatisch die E-Mail-Adresse des installierenden Benutzers in die Eigenschaften aller iQ.Suite Servers als Adresse in folgende Felder eingetragen (kann im Setup geändert werden):

- **Administrator(en)** (der iQ.Suite)
- **Antwort an** (Empfänger der Antworten auf iQ.Suite Benachrichtigungen)

2. siehe auch "Komprimierte Dateien/Archive: Der iQ.Suite Entpacker" auf Seite 76
3. siehe auch "iQ.Suite Monitor" auf Seite 123

Im Feld **Benachrichtigung von** wird der Absender von iQ.Suite Benachrichtigungen eingetragen. Dabei wird die Adresse des installierenden Benutzers wie im folgenden Screenshot gezeigt modifiziert.



Während der Installation wird außerdem die aktuelle Domäne (primäre SMTP-Adresse des installierenden Benutzers) automatisch als interne Domäne eingetragen. Um eine andere Domäne als die aktuelle einzutragen, tragen Sie hier unter **Interne Domänen** die richtige/n Domäne/n ein. Wollen Sie mehrere Domänen angeben, so werden diese mit Return voneinander getrennt. Subdomänen werden automatisch eingebunden, wenn sie mit Wildcards eingetragen werden, z.B. **.domain.com*.

Diese Einträge gelten für **alle** iQ.Suite Server. Die Einstellungen können an dieser Stelle jederzeit geändert werden.

4.5.2 Virenscanner aktiv setzen

Wählen Sie **Utility-Einstellungen --> Virenscanner** und doppelklicken Sie im rechten Fenster auf jeden Virenscanner, den Sie auf dem iQ.Suite Server instal-

liert haben, um diese mit der iQ.Suite zu verwenden. Alle Virenscanner sind vorkonfiguriert. Setzen Sie die Option **Aktiv** auf **Ja**.

Die genaue Beschreibung der Parameter entnehmen Sie bitte der Dokumentation Ihres Virenscanners. Eine Liste der Returncodes finden Sie auf der Registerkarte **Details** des jeweiligen Virenscanners. Beachten Sie die besondere Konfiguration des Virenscanners für das Pattern Update, falls Sie einen Proxy-Server verwenden!

Sollten Sie Ihren Virenscanner nicht in der Liste finden, setzen Sie sich bitte mit unserem Support in Verbindung.

Testen Sie, ob Ihr Virenscanner korrekt arbeitet: Markieren Sie unter **iQ.Suite Monitor** den gewünschten Servernamen und klicken Sie im rechten Fenster auf **Server Status**. Unter der Registerkarte **Virenscanner-Test** klicken Sie auf die Schaltfläche **Test starten**. Bei Erfolg erhalten Sie ein OK und die Meldung, dass ein EICAR Test Virus gefunden wurde.

Die nähere Beschreibung der einzelnen Virenscanner-Konfigurationen entnehmen Sie bitte dem Kapitel “Virenscanner konfigurieren” auf Seite 216.

4.5.3 Jobs aktiv schalten

Schalten Sie alle Jobs, die Sie laut Unternehmensrichtlinien verwenden möchten, aktiv. Siehe hierzu “Richtlinien-Konfiguration” auf Seite 19.

5 Installation

5.1 Systemvoraussetzungen

Für die Installation der iQ.Suite sind folgende Voraussetzungen erforderlich:

- CD-ROM-Laufwerk oder Netzwerkzugang
- RAM: Exchange-Empfehlung und zusätzlich 64 MB
- Hard Disk: 50 MB für jedes Modul
- 100 MB für Protokollierung empfohlen
- Betriebssysteme:
  - Windows 2000 Server ab Service Pack 2
  - Windows 2000 Advanced Server ab Service Pack 2
  - Windows Server 2003
- Exchange-Server:
  - MS Exchange Server 2000 ab Service Pack 2
  - MS Exchange Server 2000 Enterprise Edition ab Service Pack 2
  - MS Exchange Server 2003
- Benutzerberechtigungen
  - Im Active Directory angemeldeter Benutzer mit Administrationsrechten auf das Active Directory

Deaktivieren Sie in jedem Fall eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virenscanner für das Verzeichnis `..\iQ.Suite\GrpData`!

5.2 Vorbereitungen

5.2.1 Installation der Virenscanner

Während der Installation der iQ.Suite kann der Virenscanner AntiVir von H+BEDV installiert werden. Der AntiVir Virenscanner ist fertig konfiguriert und sofort einsatzfähig. Dazu stellen wir einen Job für die Virenprüfung mit AntiVir zur Verfügung, den Sie einfach aktivieren können.

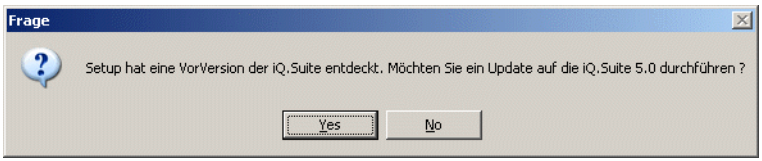
Alle anderen Virenscanner werden nicht von uns ausgeliefert. Wollen Sie einen anderen Virenscanner als AntiVir einsetzen, installieren Sie diesen bitte vor dem ersten Einsatz der iQ.Suite auf Ihrem Server! Siehe dazu auch "Virenscanner konfigurieren" auf Seite 216.

5.2.2 Update von iQ.Suite 3.x oder 4 auf Version 5

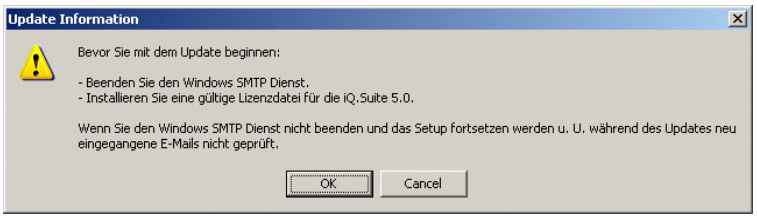
Ein Update auf Version 5 installiert die neue Version, behält dabei aber Ihre früheren Daten und Konfiguration.

Folgen Sie bitte unbedingt den Anweisungen des Setups und deinstallieren Sie **auf keinen Fall** Ihre vorherige Version. Ihre frühere Konfiguration und die Quarantäne-Daten könnten ansonsten verloren gehen!

Sie erhalten vor der Installation folgende Meldungen:



Bestätigen Sie die Meldung mit **Ja**.


Update Information
Bevor Sie mit dem Update beginnen:
- Beenden Sie den Windows SMTP Dienst.
- Installieren Sie eine gültige Lizenzdatei für die iQ.Suite 5.0.
Wenn Sie den Windows SMTP Dienst nicht beenden und das Setup fortsetzen werden u. U. während des Updates neu eingegangene E-Mails nicht geprüft.
OK
Cancel

Klicken Sie **OK** und führen Sie die angegebenen Anweisungen durch.

Bei einem Update wird der Pfad Ihres bisherigen **GrpData**-Verzeichnisses übernommen. Bei einer Neuinstallation dagegen würde der Pfad folgendermaßen gesetzt:

```
c:\Program Files\GROUP Technologies\iQ.Suite\GrpData
```

Für die deutsche Installation:

```
c:\Programme\GROUP Technologies\iQ.Suite\GrpData
```

Achten Sie darauf, dass Sie ausreichend freien Plattenplatz auf dem Laufwerk haben (je nach Mailaufkommen)!

Beim Update haben Sie die Möglichkeit, Ihre bisherigen Konfigurationseinstellungen zu übernehmen. Wählen Sie bei einem Update Ihre bisherige **ConfigData.xml** aus. Das Update der Konfiguration auf die Version 5 erfolgt automatisch beim erstmaligen Öffnen der iQ.Suite Konsole.

Haben Sie mehrere iQ.Suite Server, die sich eine Konfigurationsdatei teilen, so gehen Sie folgendermaßen vor:

1. Installieren Sie das Update **auf dem ersten Server** gemäß Anleitung unter "Installation der iQ.Suite auf mehreren Exchange-Servern" auf Seite 31. Wählen Sie bei der Installation Ihre bisherige **ConfigData.xml** aus der früheren Version aus.
2. Installieren Sie auf **allen anderen Servern** die Serverkomponente gemäß Anleitung unter "Installation der Serverkomponenten auf den Servern" auf Seite 33, **bevor Sie das erste Mal die iQ.Suite Konsole öffnen**.
3. Die **ConfigData.xml** wird beim Öffnen an die iQ.Suite 5 angepasst. Ihre bisherige Konfiguration wird übernommen.

5.3 Durchführung

5.3.1 Installation der iQ.Suite auf einem Exchange-Server

Diese Installation setzt einen betriebsbereiten Exchange Server voraus, auf dem sowohl die Serverkomponente als auch die iQ.Suite Konsole (Administration) installiert wird!

Rufen Sie aus dem Installationspaket die Datei **setup_iqsuite_msx_de.exe** mit einem Doppelklick auf.

Wenn Sie Microsoft Windows XP Service Pack 2 installiert und den Download des iQ.Suite Setup mit dem Internet Explorer durchgeführt haben, erscheint beim Setup-Start eine Sicherheitswarnung wegen einer fehlenden digitalen Signatur. Der Prozess der Herstellung digitaler Signaturen nimmt eine gewisse Zeit in Anspruch, so dass auch verlässliche Softwareanwendungen in einer Übergangsperiode nicht verifiziert sind. Sie können die Meldung ignorieren, indem Sie das Setup weiter ausführen.

Akzeptieren Sie die Lizenzbedingungen, um fortfahren zu können. Wir empfehlen, wenn möglich die Standardverzeichnisstrukturen zu verwenden. Das Standardverzeichnis für die Installation der iQ.Suite ist

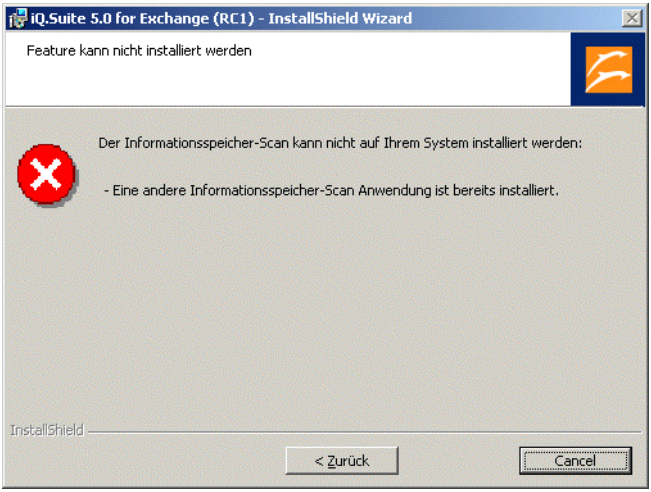
`C:\Program Files\GROUP Technologies\iQ.Suite\` (englisch)

`c:\Programme\GROUP Technologies\iQ.Suite\GrpData` (deutsch)

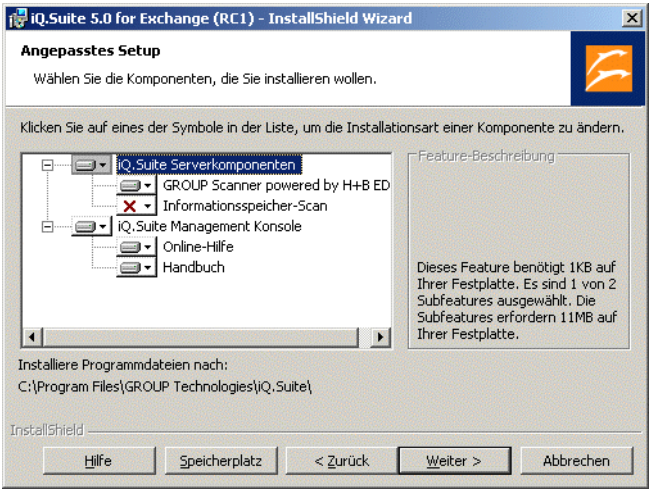
iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Angepasstes Setup
Wählen Sie die Komponenten, die Sie installieren wollen.
Klicken Sie auf eines der Symbole in der Liste, um die Installationsart einer Komponente zu ändern.
iQ.Suite Serverkomponenten
GROUP Scanner powered by H+B ED
Informationsspeicher-Scan
iQ.Suite Management Konsole
Online-Hilfe
Handbuch
Feature-Beschreibung
Dieses Feature benötigt 1KB auf Ihrer Festplatte. Es sind 2 von 2 Subfeatures ausgewählt. Die Subfeatures erfordern 22MB auf Ihrer Festplatte.
Installiere Programmdateien nach:
C:\Program Files\GROUP Technologies\iQ.Suite\
Ändern...
InstallShield
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

Klicken Sie **Weiter**. Damit werden alle Serverkomponenten und die iQ.Suite Konsole installiert.

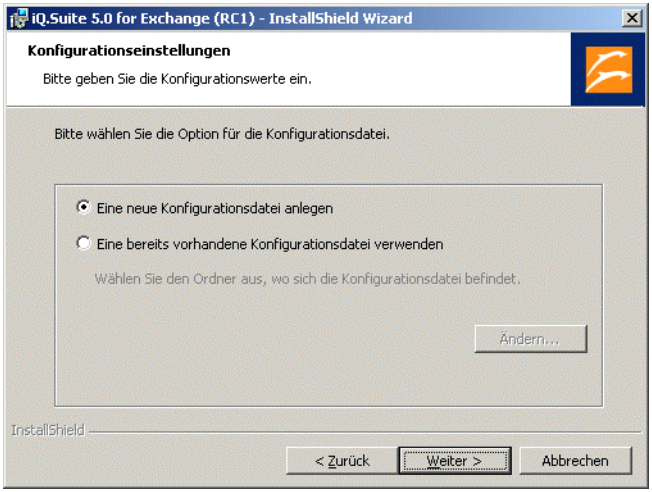
Sollte auf dem Server bereits eine andere Informationsspeicher-Scan-Anwendung laufen, erhalten Sie folgende Meldung:


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Feature kann nicht installiert werden
Der Informationsspeicher-Scan kann nicht auf Ihrem System installiert werden:
- Eine andere Informationsspeicher-Scan Anwendung ist bereits installiert.
InstallShield
< Zurück
Cancel

Klicken Sie in diesem Fall **Zurück** und deaktivieren Sie den Informationsspeicher-Scan:


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Angepasstes Setup
Wählen Sie die Komponenten, die Sie installieren wollen.
Klicken Sie auf eines der Symbole in der Liste, um die Installationsart einer Komponente zu ändern.
iQ.Suite Serverkomponenten
GROUP Scanner powered by H+B ED
Informationsspeicher-Scan
iQ.Suite Management Konsole
Online-Hilfe
Handbuch
Feature-Beschreibung
Dieses Feature benötigt 1KB auf Ihrer Festplatte. Es sind 1 von 2 Subfeatures ausgewählt. Die Subfeatures erfordern 11MB auf Ihrer Festplatte.
Installiere Programmdateien nach:
C:\Program Files\GROUP Technologies\iQ.Suite\
InstallShield
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

Wählen Sie im nächsten Fenster die Option **Eine neue Konfigurationsdatei anlegen**:


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Konfigurationseinstellungen
Bitte geben Sie die Konfigurationswerte ein.
Bitte wählen Sie die Option für die Konfigurationsdatei.
Eine neue Konfigurationsdatei anlegen
Eine bereits vorhandene Konfigurationsdatei verwenden
Wählen Sie den Ordner aus, wo sich die Konfigurationsdatei befindet.
Ändern...
InstallShield
< Zurück
Weiter >
Abbrechen

Klicken Sie **Weiter**.

iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Konfigurationseinstellungen
Bitte geben Sie die Konfigurationswerte ein.
Server:
VPC001
Sie können den Server später noch unter Basis Konfiguration / iQ.Suite Servers ändern. Weitere Informationen finden Sie im Handbuch oder in der Online-Hilfe.
E-Mail-Adresse des Administrators:
Administrator@company.com
Sie können die E-Mail-Adresse des Administrators später noch unter Basis Konfiguration / iQ.Suite Servers ändern. Weitere Informationen finden Sie im Handbuch oder in der Online-Hilfe.
InstallShield
< Zurück
Weiter >
Abbrechen

Überprüfen Sie die Konfigurationseinstellungen. Diese Einstellungen werden als Standardeinträge in die Konfiguration der **iQ.Suite Servers** übernommen. Näheres dazu ab “Definition der E-Mail-Adressen und internen Domänen” auf Seite 21

Klicken Sie **Weiter**. Evtl. erhalten Sie nun folgende Meldung:

Information
Die iQ.Suite installiert den Eicar-Test-Virus. Ein On-Access Virenscanner wird diesen Virus beim ersten Aufruf der iQ.Suite feststellen. Deaktivieren Sie deshalb nach der Installation die Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virenscanner für das Verzeichnis "C:\Program Files\GROUP Technologies\iQ.Suite\GrpData\".
OK

Deaktivieren Sie jetzt die On-Access-Scanner für das Verzeichnis `..\GrpData` und bestätigen Sie die Meldung mit **OK**. Folgen Sie weiter den Anweisungen des InstallShield Wizard und klicken Sie auf **Installieren**. Anschließend wird die iQ.Suite vollständig installiert. Mit dem **Fertigstellen** der letzten Dialogbox haben Sie die iQ.Suite erfolgreich installiert.

5.3.2 Installation der iQ.Suite auf mehreren Exchange-Servern

Wenn Sie die iQ.Suite auf mehreren Exchange-Servern installieren und sie von einer Workstation aus administrieren möchten, lesen Sie dieses Kapitel bitte sorgfältig durch.

Beachten Sie insbesondere den nachfolgenden Abschnitt "Wissenswertes zur Installation" auf Seite 31.

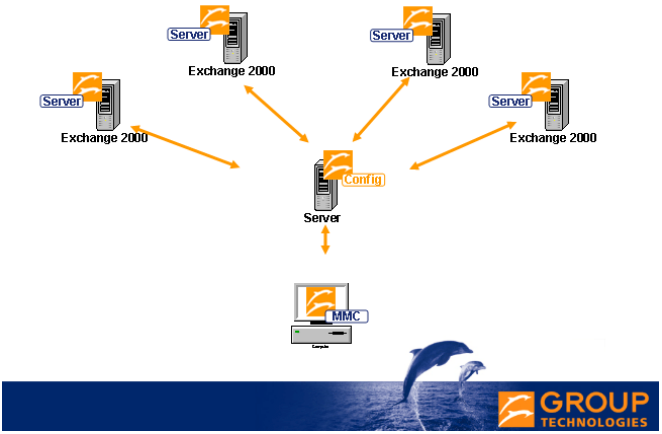
5.3.2.1 Wissenswertes zur Installation

Die iQ.Suite teilt sich architektonisch in drei Bereiche:

- MMC (iQ.Suite Konsole) = Administrationsoberfläche
  - iQ.Suite Konsole (1 MMC Snap-In)
  - Active Directory Zugriff
  - Pflege der Sicherheitsrichtlinien
  - Pflege der Quarantäne-Bereiche
  - Für Windows NT, 2000, XP, 2003
  - SOAP + SSL (z.B. „Aus Quarantäne senden")
- Server (iQ.Suite Windows Service) = Serverkomponenten (Programmdateien)
  - iQ.Suite Windows Service
  - Exchange 2000/2003 SMTP Advanced Queue Sink
  - Quarantäne-Bereiche
  - Active Directory Zugriff
  - Für Exchange 2000/2003 Frontend/Backend

- Config (iQ.Suite Konfiguration) = Die gespeicherten Unternehmensrichtlinien in individuell eingerichteten Jobs
  - iQ.Suite Konfiguration
  - XML-Datei
  - Lokales Dateisystem Netzwerk Share

Bei einer Installation auf mehreren Servern brauchen Sie auf allen Exchange-Servern die iQ.Suite Serverkomponenten und auf der Workstation, auf der Sie administrieren wollen, die iQ.Suite Konsole. Die Konfigurationsdatei muss für alle Server und für die Workstation im Zugriff gehalten werden, also zentral abgelegt sein. Der grafische Überblick:



Auf den Exchange-Servern installieren Sie nur die Serverkomponenten, auf der Administrationsworkstation installieren Sie nur die iQ.Suite Konsole und die Konfigurationsdatei legen Sie für alle Server zugänglich im Netz ab.

Auf dem ersten Server installieren Sie mindestens die Serverkomponente der iQ.Suite, damit Ihnen die Konfigurationsdatei zur Verfügung steht. Nun geben Sie den aktuellen Ordner mit der Konfigurationsdatei für alle Server frei. Dann installieren Sie die Serverkomponenten auf den restlichen Servern mit der entsprechenden Option und die iQ.Suite Konsole zusätzlich auf eine Workstation (oder auch schon vorher auf einem der Server), falls Sie lieber von dort administrieren möchten.

Der Ablauf in Einzelschritten:

1. Führen Sie auf dem ersten Server eine Installation der iQ.Suite durch (siehe "Installation der iQ.Suite auf einem Exchange-Server" auf Seite 27).
2. Starten Sie die iQ.Suite.
3. Die Konfigurationsdatei **ConfigData.xml** befindet sich nach einer vollständigen Installation im Verzeichnis
   `C:\Program Files\GROUP Technologies\iQ.Suite\Config\`
   Geben Sie diesen Ordner für alle Server frei.
4. Installieren Sie die Serverkomponenten auf den restlichen Exchange-Servern (siehe "Installation der Serverkomponenten auf den Servern" auf Seite 33) mit der Option **Eine bereits vorhandene Konfigurationsdatei verwenden**. Verweisen Sie dort auf die Datei im freigegebenen Ordner.
5. Optional: Installieren Sie die iQ.Suite Konsole auf einer Workstation, falls Sie von dort administrieren möchten (siehe "Installation der iQ.Suite Konsole auf einer Workstation" auf Seite 36) mit der Option **Eine bereits vorhandene Konfigurationsdatei verwenden**.

Halten Sie die Reihenfolge der Installationsschritte unbedingt ein!

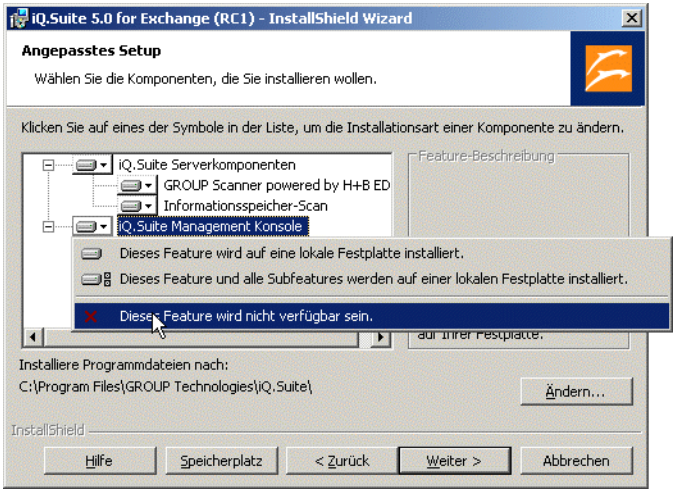
Wenn die Serverkomponenten auf mehreren Exchange-Servern laufen und Sie die iQ.Suite Konsole auf einer Workstation installieren, können Sie diese auch unter Windows NT/2000/XP betreiben. Die Workstation benötigt außerdem keinen Exchange-Server.

5.3.2.2 Installation der Serverkomponenten auf den Servern

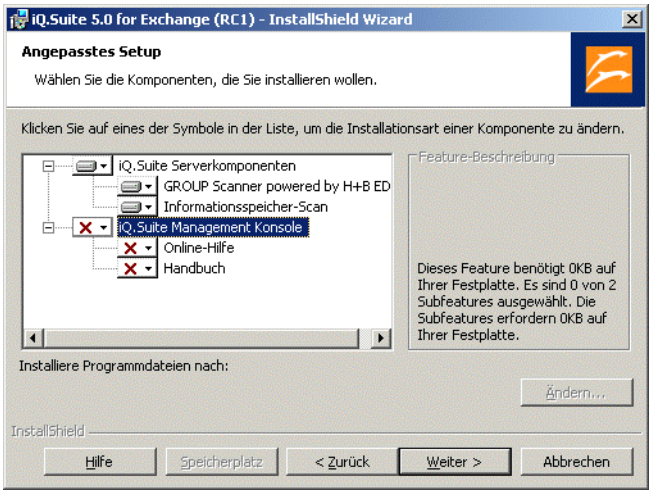
Für den ersten Exchange-Server führen Sie bitte eine Installation wie in "Installation der iQ.Suite auf einem Exchange-Server" auf Seite 27 beschrieben, damit Ihnen die Konfigurationsdatei zur Verfügung steht.

Für alle anderen Server rufen Sie aus dem Installationspaket die Datei **setup_iqsuite_msx_de.exe** mit einem Doppelklick auf.

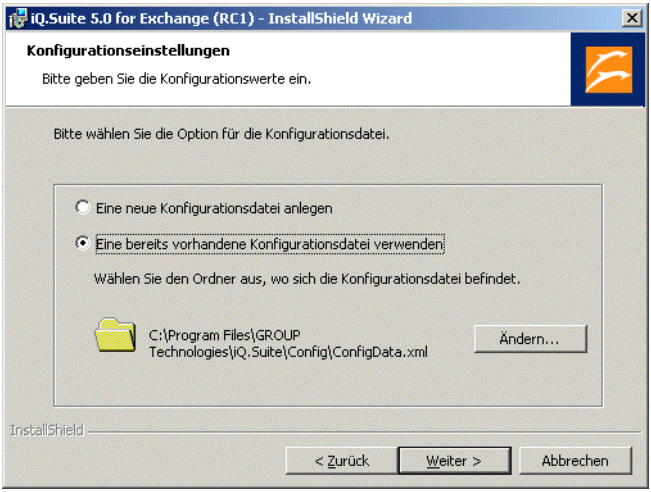
Folgen Sie den Anweisungen des InstallShield Wizard. Akzeptieren Sie die Lizenzbedingungen, um fortfahren zu können. Sie erhalten einen Dialog, in dem Sie einzelnen Komponenten auswählen können. Deaktivieren Sie die **iQ.Suite Management Konsole**:


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Angepasstes Setup
Wählen Sie die Komponenten, die Sie installieren wollen.
Klicken Sie auf eines der Symbole in der Liste, um die Installationsart einer Komponente zu ändern.
iQ.Suite Serverkomponenten
GROUP Scanner powered by H+B ED
Informationsspeicher-Scan
iQ.Suite Management Konsole
Feature-Beschreibung
Dieses Feature wird auf eine lokale Festplatte installiert.
Dieses Feature und alle Subfeatures werden auf einer lokalen Festplatte installiert.
Dieses Feature wird nicht verfügbar sein.
Installiere Programmdateien nach:
C:\Program Files\GROUP Technologies\iQ.Suite\
Ändern...
InstallShield
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

Anschließend erhalten Sie folgendes Bild:

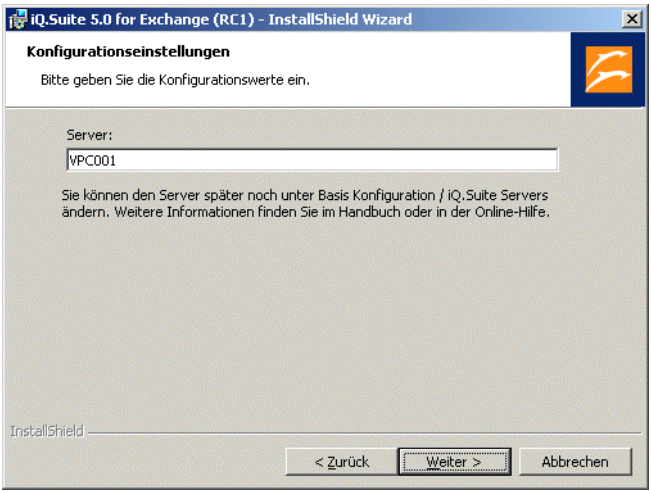

iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Angepasstes Setup
Wählen Sie die Komponenten, die Sie installieren wollen.
Klicken Sie auf eines der Symbole in der Liste, um die Installationsart einer Komponente zu ändern.
iQ.Suite Serverkomponenten
GROUP Scanner powered by H+B ED
Informationsspeicher-Scan
iQ.Suite Management Konsole
Online-Hilfe
Handbuch
Feature-Beschreibung
Dieses Feature benötigt 0KB auf Ihrer Festplatte. Es sind 0 von 2 Subfeatures ausgewählt. Die Subfeatures erfordern 0KB auf Ihrer Festplatte.
Installiere Programmdateien nach:
Ändern...
InstallShield
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

Klicken Sie **Weiter**.


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Konfigurationseinstellungen
Bitte geben Sie die Konfigurationswerte ein.
Bitte wählen Sie die Option für die Konfigurationsdatei.
Eine neue Konfigurationsdatei anlegen
Eine bereits vorhandene Konfigurationsdatei verwenden
Wählen Sie den Ordner aus, wo sich die Konfigurationsdatei befindet.
C:\Program Files\GROUP Technologies\iQ.Suite\Config\ConfigData.xml
Ändern...
InstallShield
< Zurück
Weiter >
Abbrechen

Wählen Sie die Option **Eine bereits vorhandene Konfigurationsdatei verwenden**. Klicken Sie **Ändern**. Jetzt wählen Sie den Pfad Ihrer Konfigurationsdatei (Die **ConfigData.xml** aus Ihrer vollständigen Installation):

Nachdem Sie das Verzeichnis für die Daten gewählt haben, überprüfen Sie den Servernamen. Alle weiteren Informationen werden aus der bisherigen Konfiguration übernommen.


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Konfigurationseinstellungen
Bitte geben Sie die Konfigurationswerte ein.
Server:
VPC001
Sie können den Server später noch unter Basis Konfiguration / iQ.Suite Servers ändern. Weitere Informationen finden Sie im Handbuch oder in der Online-Hilfe.
InstallShield
< Zurück
Weiter >
Abbrechen

Klicken Sie Weiter und dann auf **Installieren**. Anschließend werden die Serverkomponenten der iQ.Suite installiert.

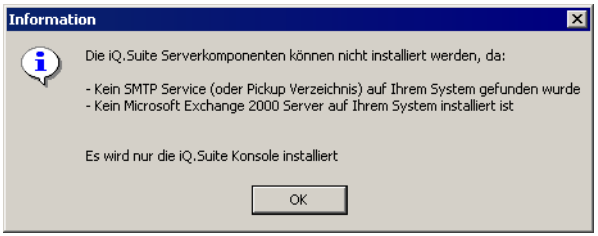
Mit dem **Fertigstellen** der letzten Dialogbox ist die Installation der Serverkomponenten abgeschlossen.

Wiederholen Sie diese Installation für jeden Exchange-Server, den Sie in der Konfiguration eingetragen haben.

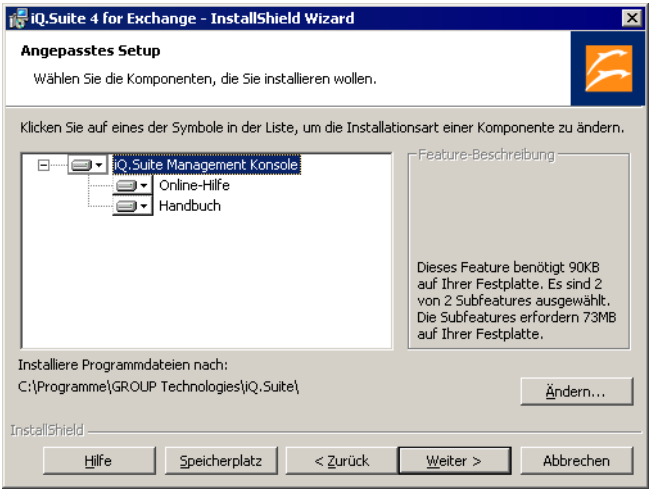
5.3.2.3 Installation der iQ.Suite Konsole auf einer Workstation

Die iQ.Suite Konsole auf der Workstation können Sie auch unter Windows NT/2000/XP betreiben. Die Workstation benötigt außerdem keinen Exchange-Server.

Für die Installation der iQ.Suite Konsole rufen Sie **setup_iqsuite_msx_de.exe** auf. Gehen Sie analog zur Installation der Serverkomponenten vor. Sie erhalten zunächst eine Meldung, wenn kein Exchange-Server installiert ist:

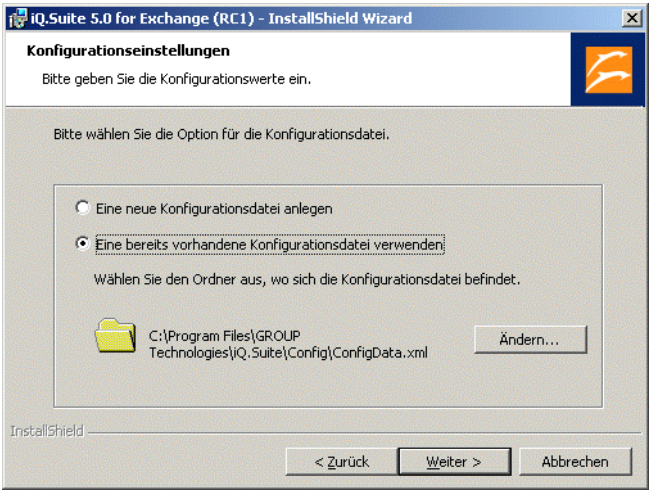

Information
Die iQ.Suite Serverkomponenten können nicht installiert werden, da:
- Kein SMTP Service (oder Pickup Verzeichnis) auf Ihrem System gefunden wurde
- Kein Microsoft Exchange 2000 Server auf Ihrem System installiert ist
Es wird nur die iQ.Suite Konsole installiert
OK

Klicken Sie **OK**. Im nächsten Dialog werden die Serverkomponenten als nicht zu installierende Features markiert.


iQ.Suite 4 for Exchange - InstallShield Wizard
Angepasstes Setup
Wählen Sie die Komponenten, die Sie installieren wollen.
Klicken Sie auf eines der Symbole in der Liste, um die Installationsart einer Komponente zu ändern.
iQ.Suite Management Konsole
Online-Hilfe
Handbuch
Feature-Beschreibung
Dieses Feature benötigt 90KB auf Ihrer Festplatte. Es sind 2 von 2 Subfeatures ausgewählt. Die Subfeatures erfordern 73MB auf Ihrer Festplatte.
Installiere Programmdateien nach:
C:\Programme\GROUP Technologies\iQ.Suite\
Ändern...
InstallShield
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

Sie installieren jetzt nur die Konsole. Klicken Sie **Weiter**.

Im nächsten Dialog werden Sie aufgefordert, die aktuelle Konfigurationsdatei auszuwählen:


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Konfigurationseinstellungen
Bitte geben Sie die Konfigurationswerte ein.
Bitte wählen Sie die Option für die Konfigurationsdatei.
Eine neue Konfigurationsdatei anlegen
Eine bereits vorhandene Konfigurationsdatei verwenden
Wählen Sie den Ordner aus, wo sich die Konfigurationsdatei befindet.
C:\Program Files\GROUP Technologies\iQ.Suite\Config\ConfigData.xml
Ändern...
InstallShield
< Zurück
Weiter >
Abbrechen

Klicken Sie **Ändern** und geben Sie das Verzeichnis an, in dem Sie Ihre Konfigurationsdatei (**ConfigData.xml**) abgelegt haben.

Klicken Sie **Weiter**. Überprüfen Sie im nächsten Dialog die Konfigurationseinstellungen. Anschließend beginnt die Installation.

Mit dem **Fertigstellen** der letzten Dialogbox ist die Installation der iQ.Suite Konsole auf der Workstation abgeschlossen.

5.4 Deinstallation der iQ.Suite 5 für Exchange

Klicken Sie auf

und wählen Sie **Einstellungen --> Systemsteuerung --> Software**. **Entfernen** Sie die **GROUP Technologies iQ.Suite 5**.

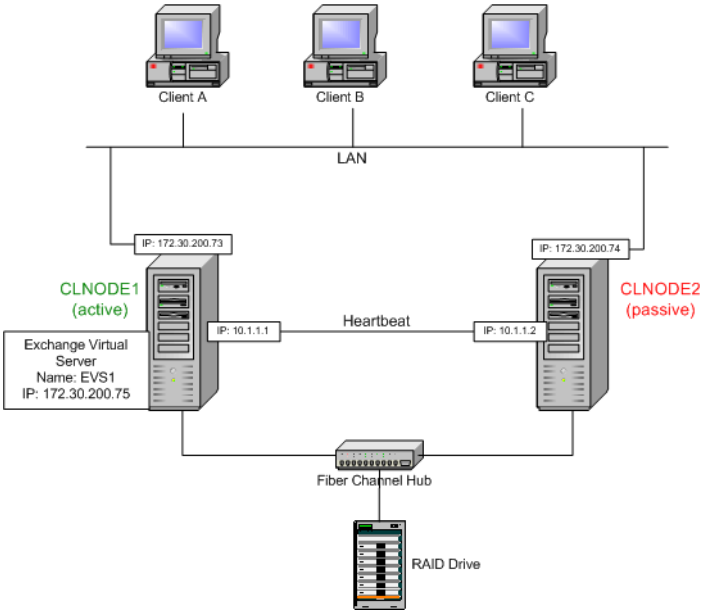
5.5 Erstinstallation für MS Active/Passive Cluster-Server

5.5.1 Installationsschritte

Die Installation der iQ.Suite auf einem Microsoft Cluster-Server (im Weiteren nur Cluster genannt) kann in vier Schritte unterteilt werden:

1. Lokale Installation der iQ.Suite auf allen Knoten (=Nodes) im Cluster.
2. Anpassen der aktiven Knoten:
   a) Kopieren des **GrpData**- und **Config**-Verzeichnisses,
   b) Anpassen der Registry,
   c) Anpassen des ToolServer in der Konfiguration.
3. Einrichten des iQ.Suite Service als Cluster-Ressource in allen Exchange Virtual Server Gruppen mit Hilfe des Cluster Administrators.
4. Aktivieren des Grabbers auf den aktiven Knoten.

Die Installation wird hier am Beispiel des folgenden 2-Knoten-Active/Passive-Cluster durchgeführt:



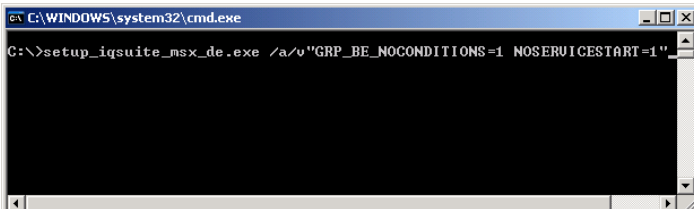
Der Knoten „CLNODE1“ wurde als aktiver Knoten eingerichtet, d.h. auf ihr läuft im Normalfall der Exchange Virtual Server „EVS1“. Dieser speichert seine Logdateien und Datenbasis auf der Disk-Resource „Disk N:“ des Clusters. Im Failover-Fall wird der Exchange Virtual Server EVS1 auf CLNODE2 übertragen.

5.5.2 Lokale Installation der iQ.Suite

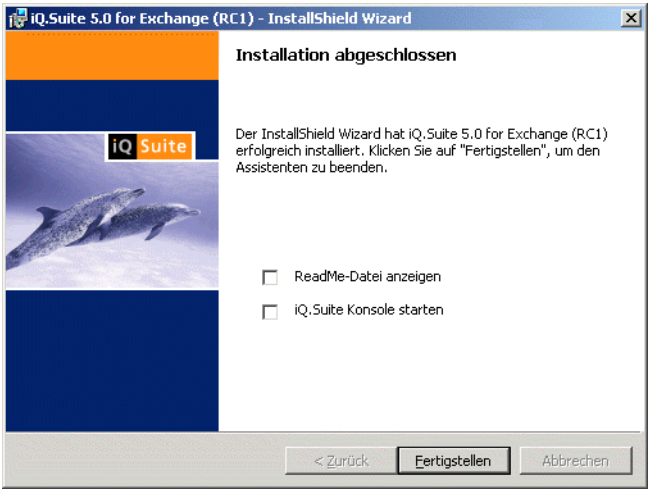
Die folgenden beschriebenen Schritte müssen auf allen Knoten (aktiven und passiven) durchgeführt werden.

1. Starten Sie die **setup_iqsuite_msx_de.exe** der iQ.Suite per Kommandozeile:

   setup_iqsuite_msx_de.exe /a/v"GRP_BE_NOCONDITIONS=1 NOSERVICESTART=1"



2. Die weiteren Schritte der lokalen Installation der iQ.Suite sind die gleichen wie bei der Installation im NICHT-Cluster-Fall (siehe "Installation der iQ.Suite auf einem Exchange-Server" auf Seite 27, Ausnahme: **Frontend hier nicht starten, deaktivieren Sie die beiden Optionen wie hier im Screenshot gezeigt!**).


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Installation abgeschlossen
iQ Suite
Der InstallShield Wizard hat iQ.Suite 5.0 for Exchange (RC1) erfolgreich installiert. Klicken Sie auf "Fertigstellen", um den Assistenten zu beenden.
ReadMe-Datei anzeigen
iQ.Suite Konsole starten
< Zurück
Fertigstellen
Abbrechen

5.5.3 Anpassen der aktiven Knoten

In der weiteren Beschreibung wird davon ausgegangen, dass beim Setup die Defaultwerte für Pfade übernommen werden (`C:\Program Files\Group Technologies\iQ.Suite` für die englische und `C:\Programme\Group Technologies\iQ.Suite` für die deutsche Installation).

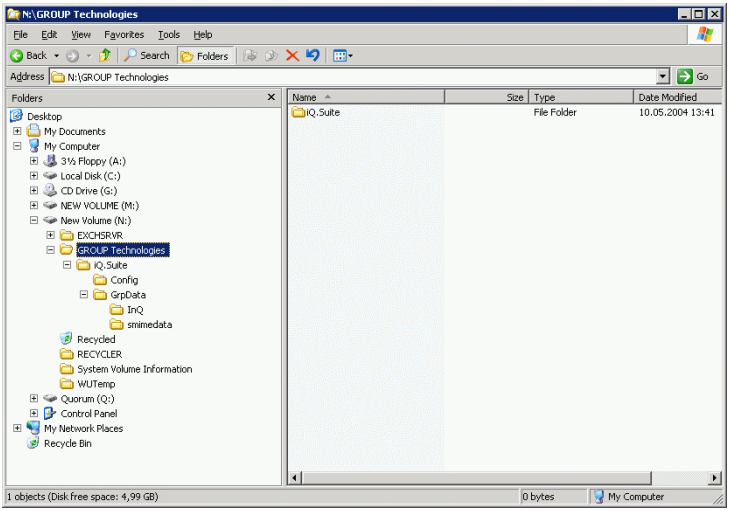
5.5.3.1 Kopieren des GrpData- und Config-Verzeichnisses

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

Kopieren Sie die Verzeichnisse

- `C:\Program Files\GROUP Technologies\iQ.Suite\GrpData`
- `C:\Program Files\GROUP Technologies\iQ.Suite\Config`

auf die Disk-Resource des Exchange Virtual Server des jeweiligen Knoten. In unserem Fall ist dies das Laufwerk `N:`. Wir legen hier einen Ordner *GROUP Technologies* an, in den die Unterverzeichnisse `iQ.Suite\GrpData` und `iQ.Suite\Config` aus `C:\Program Files\GROUP Technologies` kopiert werden.

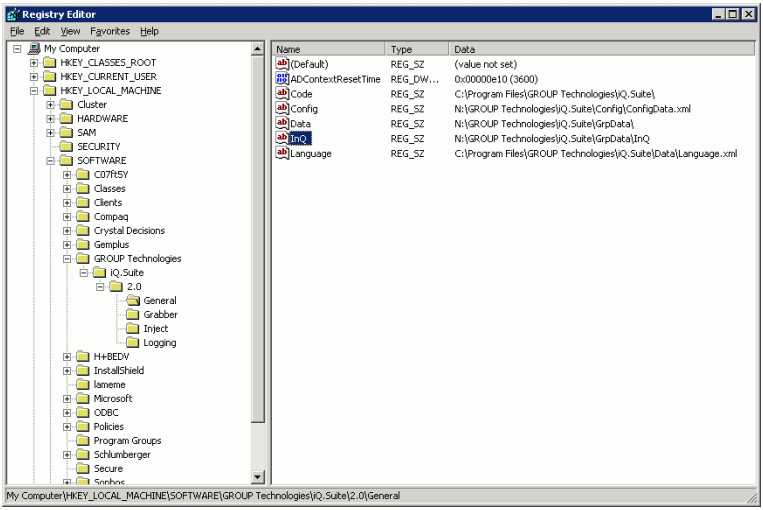


5.5.3.2 Anpassen der Registry

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

Passen Sie die Registry entsprechend der kopierten Verzeichnisse in "Kopieren des GrpData- und Config-Verzeichnisses" auf Seite 40 an:

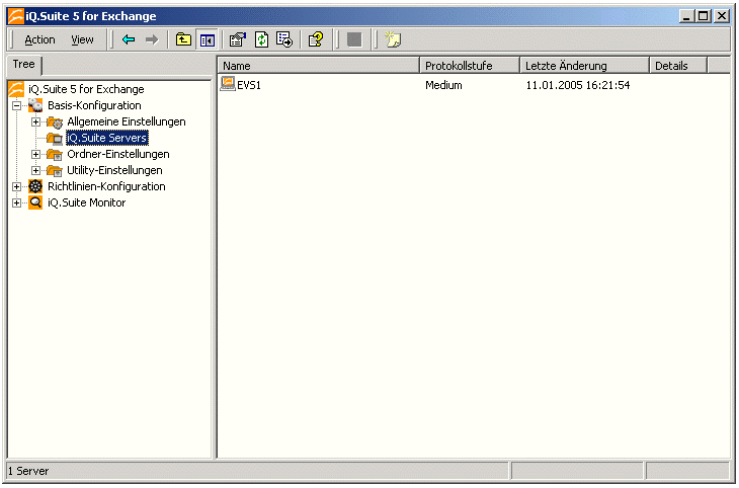
```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
General]
"Data"="N:\GROUP Technologies\iQ.Suite\GrpData\"
"Config"="N:\GROUP Technologies\iQ.Suite\Config\ConfigData.xml"
"InQ"="N:\GROUP Technologies\iQ.Suite\GrpData\InQ"
```



5.5.3.3 Anpassen der iQ.Suite Konfigurationsdatei

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

Tragen Sie in den Konfigurationsdateien auf den aktiven Knoten die entsprechenden Exchange Virtual Server (EVS) des aktiven Knotens als iQ.Suite-Server ein. In unserem Beispiel wäre das *EVS1*. Die während des Setups eingetragenen Namen der Clusterknoten können Sie aus der Konfiguration löschen.



5.5.4 Kopieren der Lizenzdateien auf alle Knoten

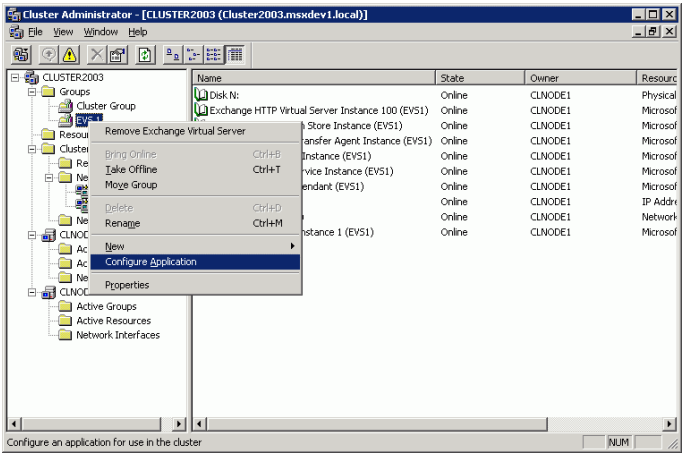
Kopieren Sie auf alle Knoten im Cluster die gültigen Lizenzdateien in das Verzeichnis `..\iQ.Suite\License`.

5.5.5 Einrichten der iQ.Suite als Cluster-Ressource

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

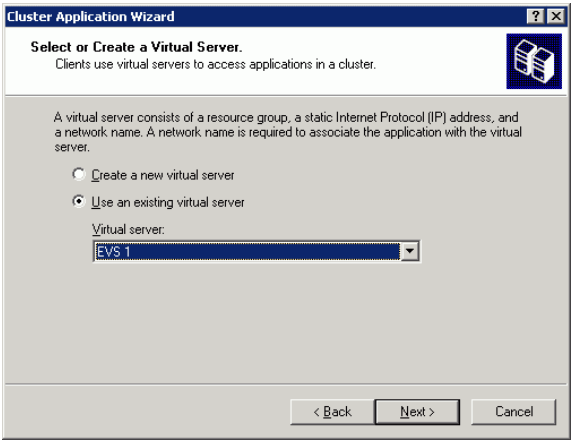
Richten Sie mit dem Cluster-Administrator den iQ.Suite Service als „Generic Service“ ein. Dies muss jeweils auf den aktiven Knoten durchgeführt werden, auf denen auch ein Exchange Virtual Server läuft. In unserem Fall führen wir dies auf CLNODE1 durch.

1. Öffnen Sie den **Cluster Administrator**.
   Klicken Sie mit der rechten Maustaste auf Exchange Virtual Server **EVS 1** --> **Configure Application**.



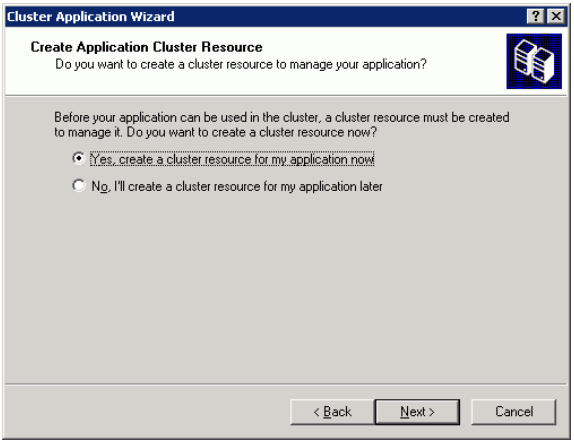
2. Klicken Sie im Begrüßungsfenster des Assistenten **Welcome to the Cluster Application Wizard** auf **Next**.
3. Dialog **Select Or Create a Virtual Server:**

   Klicken Sie auf die Option **Use an existing virtual server** und wählen Sie den entsprechenden Exchange Virtual Server aus, der auf diesem Knoten aktiv ist (hier *EVS 1*). Klicken Sie **Next**.


Cluster Application Wizard
Select or Create a Virtual Server.
Clients use virtual servers to access applications in a cluster.
A virtual server consists of a resource group, a static Internet Protocol (IP) address, and a network name. A network name is required to associate the application with the virtual server.
Create a new virtual server
Use an existing virtual server
Virtual server:
EVS 1
< Back
Next >
Cancel

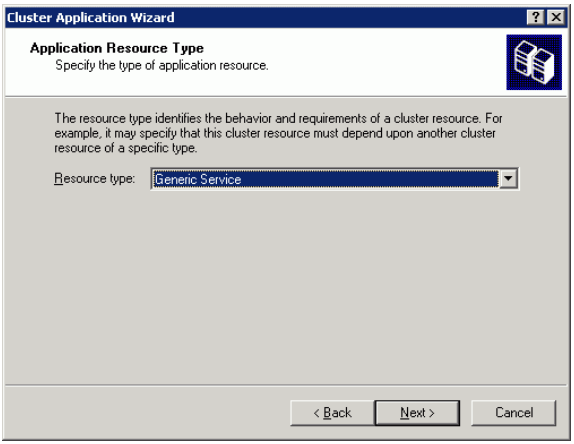
4. Dialog **Create Application Cluster Resource**:

   Wählen Sie die Option **Yes, create a cluster resource for my application now** aus und klicken Sie **Next**.


Cluster Application Wizard
Create Application Cluster Resource
Do you want to create a cluster resource to manage your application?
Before your application can be used in the cluster, a cluster resource must be created to manage it. Do you want to create a cluster resource now?
Yes, create a cluster resource for my application now
No, I'll create a cluster resource for my application later
< Back
Next >
Cancel

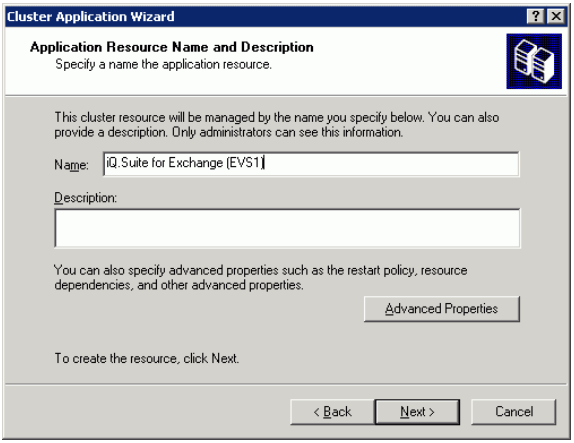
5. Dialog **Application Resource Type**:

   Wählen Sie **Resource type** *Generic Service* aus und klicken Sie **Next**.

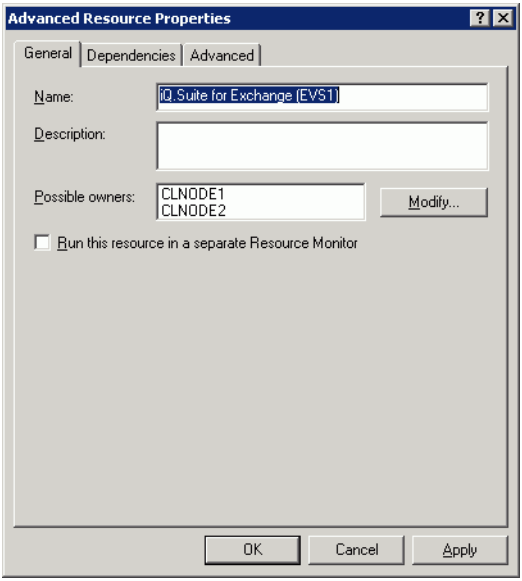

Cluster Application Wizard
Application Resource Type
Specify the type of application resource.
The resource type identifies the behavior and requirements of a cluster resource. For example, it may specify that this cluster resource must depend upon another cluster resource of a specific type.
Resource type:
Generic Service
< Back
Next >
Cancel

6. Dialog **Application Resource Name and Description**:

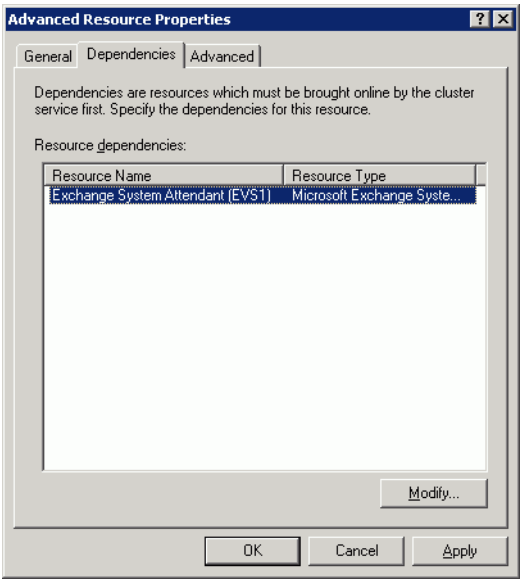
   Geben Sie bei **Name** *iQ.Suite for Exchange (EVS 1)* ein (der Name muss eindeutig im Cluster sein) und klicken Sie auf **Advance Properties**.


Cluster Application Wizard
Application Resource Name and Description
Specify a name the application resource.
This cluster resource will be managed by the name you specify below. You can also provide a description. Only administrators can see this information.
Name:
iQ.Suite for Exchange (EVS1)
Description:
You can also specify advanced properties such as the restart policy, resource dependencies, and other advanced properties.
Advanced Properties
To create the resource, click Next.
< Back
Next >
Cancel

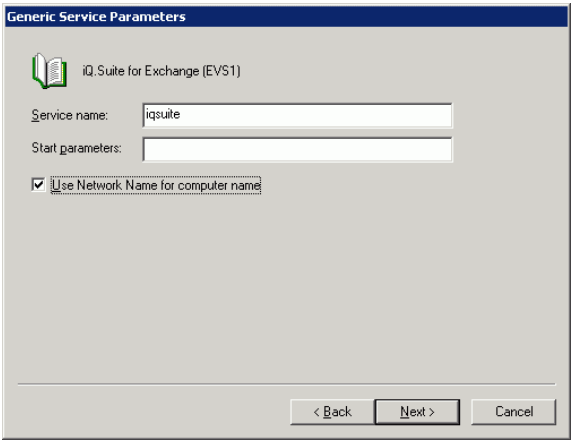
7. Auf **Advance Resource Properties**, Registerkarte **General**:
   Tragen Sie als **Possible owners** den aktiven Knoten, auf der der Exchange Virtual Server vorwiegend läuft, und den passiven Knoten ein (hier CLNODE1 und CLNODE2). Klicken Sie dann auf die Registerkarte **Dependencies**.



8. Auf **Advance Resource Properties**, Registerkarte **Dependencies**:
   Wählen Sie die über die **Modify…**-Schaltfläche die **Exchange System Attendant** Resource des EVS aus und fügen Sie sie zur Liste **Resource dependencies** hinzu. Klicken Sie **OK**.



9. Dialog **Generic Service Parameters**:
   Geben Sie bei **Service name** *iqsuite* ein und wählen Sie die Option **Use Network Name as computer name** aus. Klicken Sie **Next**.

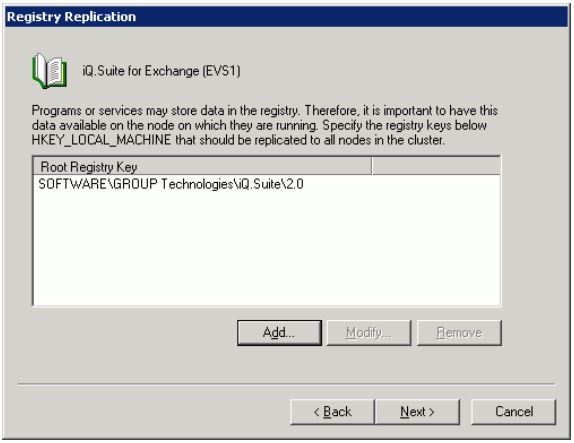


10. Dialog **Registry Replication**:

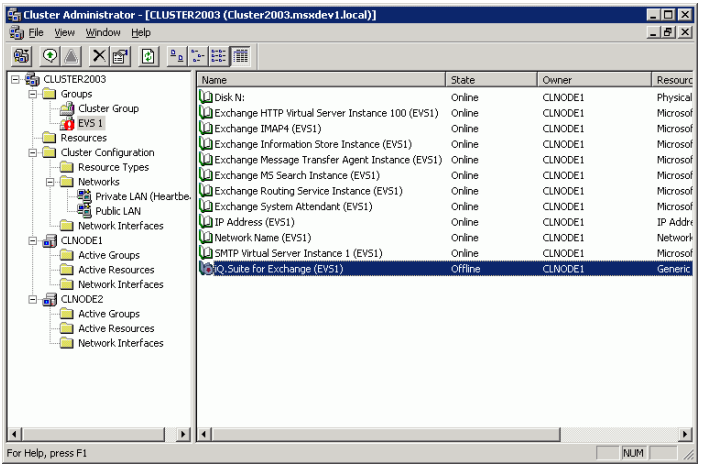
    Fügen Sie über die **Add…**-Schaltfläche den Registry Key

    `SOFTWARE\GROUP Technologies\iQ.Suite\2.0`

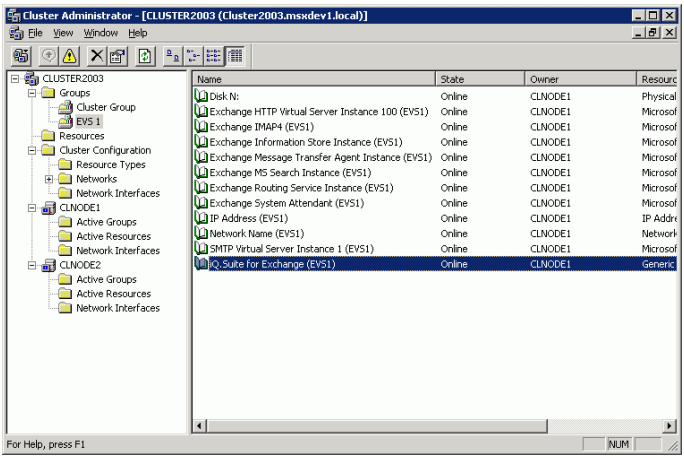
    hinzu und klicken Sie **Next**.


Registry Replication
iQ.Suite for Exchange (EVS1)
Programs or services may store data in the registry. Therefore, it is important to have this data available on the node on which they are running. Specify the registry keys below HKEY_LOCAL_MACHINE that should be replicated to all nodes in the cluster.
Root Registry Key
SOFTWARE\GROUP Technologies\iQ.Suite\2.0
Add...
Modify...
Remove
< Back
Next >
Cancel

11. Schließen Sie den nächsten Dialog **Completing the Cluster Application Wizard** mit **Finish**.
12. Der Wizard schließt sich. Die Cluster-Resource **iQ.Suite for Exchange (EVS1)** ist nun im Cluster-Administrator sichtbar, aber offline.



13. Klicken Sie mit der rechten Maustaste auf **iQ.Suite for Exchange (EVS1)** und **Bring Online** --> die Resource geht online.


Cluster Administrator - [CLUSTER2003 (Cluster2003.msxdev1.local)]
File View Window Help
CLUSTER2003
Groups
Cluster Group
EVS 1
Resources
Cluster Configuration
Resource Types
Networks
Network Interfaces
CLNODE1
Active Groups
Active Resources
Network Interfaces
CLNODE2
Active Groups
Active Resources
Network Interfaces
Name State Owner Resourc
Disk N: Online CLNODE1 Physical
Exchange HTTP Virtual Server Instance 100 (EVS1) Online CLNODE1 Microsof
Exchange IMAP4 (EVS1) Online CLNODE1 Microsof
Exchange Information Store Instance (EVS1) Online CLNODE1 Microsof
Exchange Message Transfer Agent Instance (EVS1) Online CLNODE1 Microsof
Exchange MS Search Instance (EVS1) Online CLNODE1 Microsof
Exchange Routing Service Instance (EVS1) Online CLNODE1 Microsof
Exchange System Attendant (EVS1) Online CLNODE1 Microsof
IP Address (EVS1) Online CLNODE1 IP Addr
Network Name (EVS1) Online CLNODE1 Network
SMTP Virtual Server Instance 1 (EVS1) Online CLNODE1 Microsof
IQ.Suite for Exchange (EVS1) Online CLNODE1 Generic
For Help, press F1
NUM

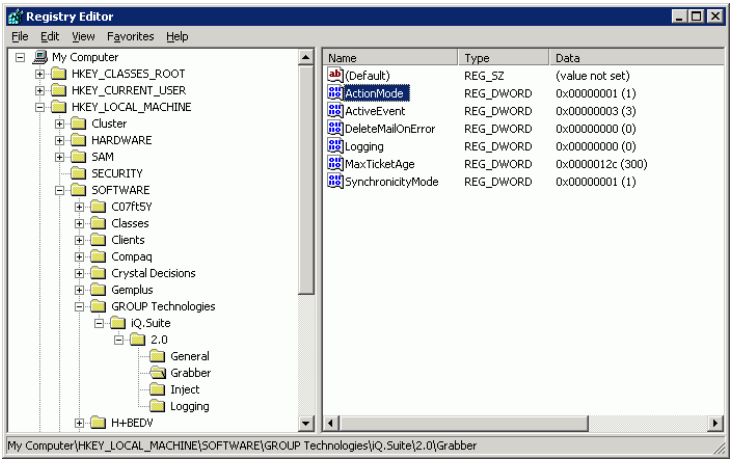
5.5.6 Aktivieren des Grabbers

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

Als letzten Schritt aktivieren Sie den Grabber. Ändern Sie zu diesem Zweck den Registry-Wert **ActionMode** in der Sektion **Grabber** der iQ.Suite Registry-Einstellungen von 0 auf 1.

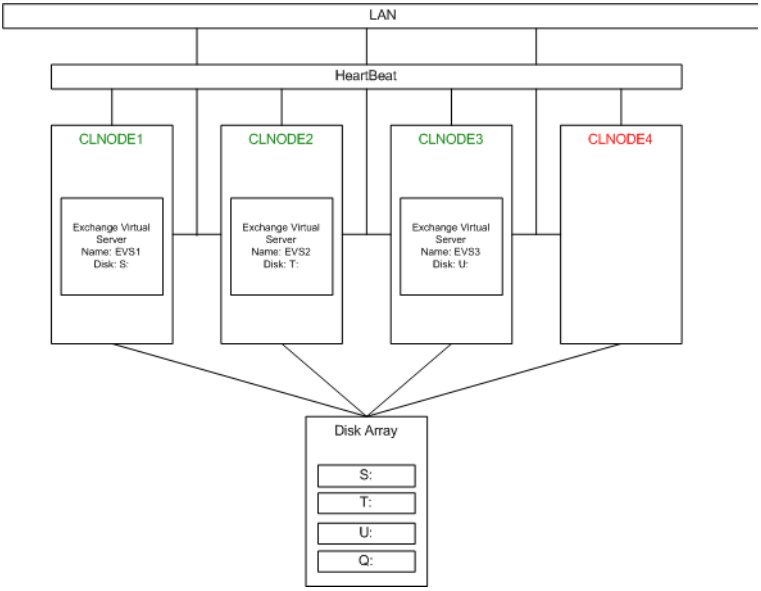
Die Cluster-Resource **iQ.Suite for Exchange (EVS1) muss** während dieses Installationsschrittes für diesen Knoten **Online** sein.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
Grabber]
"ActionMode"= dword:00000001
```



5.5.7 Beispiel einer Erstinstallation auf einem 4-Knoten-Cluster

Um die oben genannten Installationsschritte noch einmal zu verdeutlichen, werden wir die Konfiguration der iQ.Suite Resource in einem 4-Knoten-Active/Passive-Cluster beispielhaft vorstellen. Wir nehmen an, dass 3 Knoten aktiv sind und 1 Knoten passiv läuft. Grafisch dargestellt sieht das folgendermaßen aus:



CLNODE1, CLNODE2, CLNODE3 sind aktive Knoten. CLNODE4 läuft stand-by (passiv). Als Ausgangssituation ist jedem aktiven Knoten ein Exchange Virtual Server zugewiesen: EVS1, EVS2, EVS3. Ihre Knoten sind ihre „preferred owner".

Im ersten Schritt wird die iQ.Suite lokal auf jedem Knoten (CLNODE 1-4) wie in "Lokale Installation der iQ.Suite" auf Seite 39 beschrieben installiert. Bei der Registrierung des Grabbers muss beachtet werden, dass der Grabber für die richtige Instanz des SMTP-Servers auf den Knoten registriert wird, da im Cluster jeder Exchange Virtual Server mit einer eigenen Instanz eines virtuellen SMTP-Servers läuft. Die Instanznummer wird mit jedem neu installiertem Exchange Virtual Server im Cluster inkrementiert, beginnend bei 1. Die folgende Tabelle zeigt, für welche Instanzen auf welchen Knoten der Grabber registriert werden muss.

Knoten	Grabber muss registriert werden für virtuellen SMTP-Server mit der Instanznummer
CLNODE1	1
CLNODE2	2

CLNODE3	3
CLNODE4	1, 2, 3

Es ist zu erkennen, dass der Grabber auf den aktiven Knoten nur für die jeweils laufende Instanz des virtuellen SMTP-Servers registriert wird. Auf dem passiven Knoten muss der Grabber für alle Instanzen registriert werden, da im Failover-Fall jede Instanz auf diesem Knoten laufen könnte. Die Registrierung erfolgt mit dem Tool **GrabberInstaller2** oder über die Batch **registerGrabber2.bat**, wobei hier die Batch für jede Instanznummer angepasst werden muss. Damit auf dem passiven Knoten eine Registrierung für alle Instanzen des virtuellen SMTP-Servers möglich ist, kann es sein, dass jeder EVS einmal auf den passiven Knoten verschoben werden muss.

Sobald dies geschehen ist, müssen auf **jedem aktiven** Knoten die Anpassungen aus Abschnitt "Anpassen der aktiven Knoten" auf Seite 40 gemacht werden. In der nachfolgenden Übersicht sind die nötigen Anpassungen auf CLNODE1-3 aufgelistet:

CLNODE1
Verzeichnis verschoben nach: `S:`
Registry:

```
"Data"="S:\GROUP Technologies\iQ.Suite\GrpData\"
"Config"=
"S:\GROUP Technologies\iQ.Suite\Config\ConfigData.xml"
"InQ"="S:\GROUP Technologies\iQ.Suite\GrpData\InQ"
```

iQ.Suite Server in Konfiguration: EVS1, EVS2, EVS3

CLNODE2
Verzeichnis verschoben nach: `T:`
Registry:

```
"Data"="T:\GROUP Technologies\iQ.Suite\GrpData\"
"Config"=
"T:\GROUP Technologies\iQ.Suite\Config\ConfigData.xml"
"InQ"="T:\GROUP Technologies\iQ.Suite\GrpData\InQ"
```

iQ.Suite Server in Konfiguration: EVS1, EVS2, EVS3

CLNODE3
Verzeichnis verschoben nach: `U:`
Registry:

```
"Data"="U:\GROUP Technologies\iQ.Suite\GrpData\"
"Config"=
"U:\GROUP Technologies\iQ.Suite\Config\ConfigData.xml"
"InQ"="U:\GROUP Technologies\iQ.Suite\GrpData\InQ"
```

iQ.Suite Server in Konfiguration: EVS1, EVS2, EVS3

Wie man sieht, müssen die Verzeichnisse auf die Disk-Resource des jeweiligen Exchange Virtual Servers des Knotens verschoben werden. Die Registry-Einträge ändern sich damit analog. Als iQ.Suite Server werden in allen Konfigurationsdateien alle Cluster-Knoten eingetragen.

Die Einrichtung des iQ.Suite Service als Cluster-Resource muss in der jeweiligen Gruppe des Exchange Virtual Servers auf den aktiven Knoten erfolgen. Auf CLNODE1 wird also der iQ.Suite Service in der Gruppe EVS1 angelegt, auf CLNODE2 in der Gruppe EVS2 und auf CLNODE3 in der Gruppe EVS3. In der nachfolgenden Tabelle sind die Eigenschaften iQ.Suite Ressourcen auf den Cluster-Knoten dargestellt, in denen sich die iQ.Suite Ressourcen unterscheiden.

Knoten	Name	Gehört zur Gruppe	Resource dependencies	Possible Owners
CLNODE1	iQ.Suite – (EVS1)	EVS1	Exchange System Attendant (EVS1)	CLNODE1 CLNODE4
CLNODE2	iQ.Suite – (EVS2)	EVS2	Exchange System Attendant (EVS2)	CLNODE2 CLNODE4
CLNODE3	iQ.Suite – (EVS3)	EVS3	Exchange System Attendant (EVS3)	CLNODE3 CLNODE4

Die Einstellungen bzgl. **Registry Replication** und **Service name** sind in allen drei Fällen gleich. Die Namen unterscheiden sich, da sie im Cluster eindeutig sein müssen. Außerdem sind die **Resource dependencies** nicht identisch. Als

Possible Owners wurde der jeweils entsprechende aktive Knoten und zusätzlich der passive Knoten eingetragen.

Die Aktivierung des Grabbers erfolgt - wie in Abschnitt "Aktivieren des Grabbers" auf Seite 49 beschrieben - auf jedem aktiven Knoten, während die entsprechende iQ.Suite Cluster-Resource online ist.

5.6 Update von V3.x/V4.0 nach V5.0 in einem Cluster

Ein Update einer Version V3.x bzw. V4.0 der iQ.Suite für Exchange nach einer Version 5.0 wird wie folgt durchgeführt:

1. Update auf den passiven Knoten.
2. Failover des Exchange Virtual Server (EVS) auf den aktualisierten passiven Knoten.
3. Update des vormals aktiven (jetzt passiven) Knotens.
4. Fallback des EVS auf den ursprünglichen Knoten (falls erforderlich).

Mit dieser Update-Vorgehensweise wird das iQ.Suite Setup nur auf passiven Knoten durchgeführt und damit der laufende Betrieb des Exchange-Servers nicht gestört. Nur beim Failover vom aktiven auf passiven Knoten muss der SMTP-Dienst gestoppt werden. Danach kann der Exchange-Server wieder unbeeinträchtigt weiterlaufen.

Das Update der Cluster-Knoten muss „in einem Zug" erfolgen: Ein Mischbetrieb von gleichzeitig V3.5 bzw. V4.0 auf einigen Knoten und V5.0 auf anderen Knoten ist nicht möglich!

Im Folgenden stellen wir diese Schritte anhand des in Abschnitt "Erstinstallation für MS Active/Passive Cluster-Server" auf Seite 38 beschriebenen 2-Knoten-Active/Passive-Cluster vor. Auf beiden Knoten ist die iQ.Suite für Exchange V3.5 installiert. CLNODE1 ist per Default der aktive, CLNODE2 der passive Knoten. Die lokalen Installationspfade der iQ.Suite V3.5 sind
`C:\Program files\GROUP Technologies\iQ.Suite` und
`C:\GrpData`.

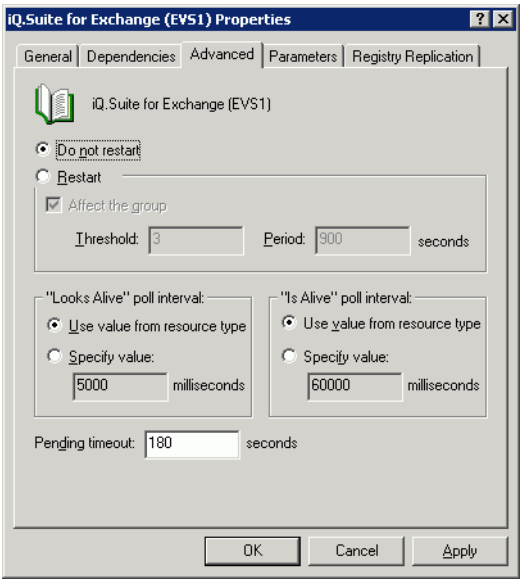
Als Installationspfade für die gemeinsamen Daten der iQ.Suite V3.5 Cluster-Resource nehmen wir folgende Pfade an:
`N:\Group Technologies\config` und

```
N:\Group Technologies\GrpData
```

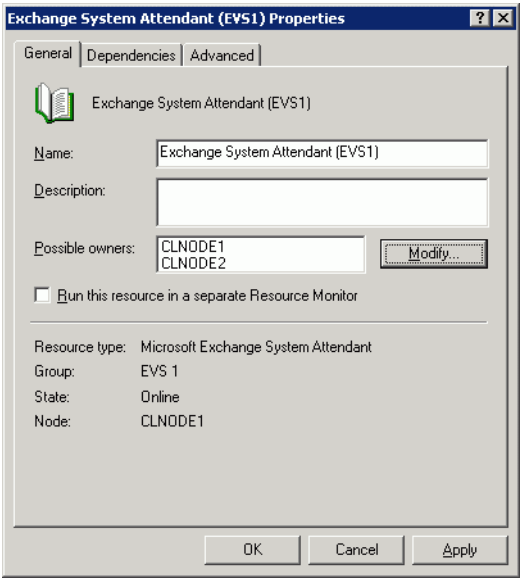
(Setzen Sie hier die Pfade Ihrer eigenen Version ein!)

5.6.1 Update der passiven Knoten CLNODE1

1. Öffnen Sie im Cluster-Administrator über die rechte Maustaste die **Properties** der iQ.Suite for Exchange-Resource und die Registerkarte **Advanced**, wählen Sie dann die Option **Do not restart**. Damit wird verhindert, dass beim einem Fehler während des Updates die ganze EVS Gruppe betroffen ist.

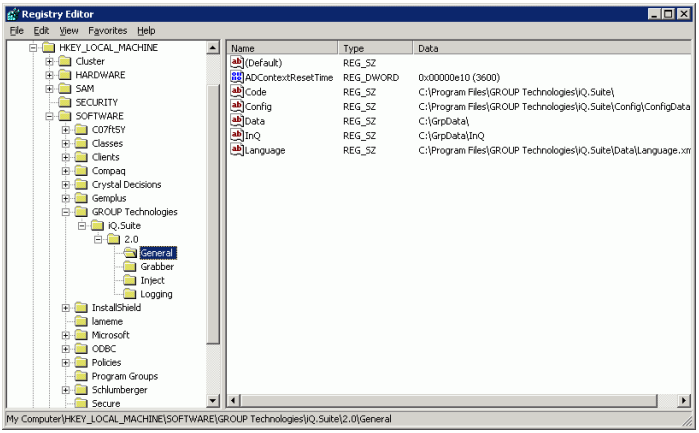


2. Um zu verhindern, dass während des Updates des passiven Knotens ein Failover auf diese auftritt, darf sie unter den **Possible owners** aller EVS im Cluster nicht mehr erscheinen. In unserem Falle heißt dies: Öffnen Sie im Cluster Administrator über die rechte Maustaste die **Properties** der Resource **Exchange System Attendant**, wählen Sie die Registerkarte **General** und entfernen Sie CLNODE2 aus **Possible owners** (über **Modify...**).

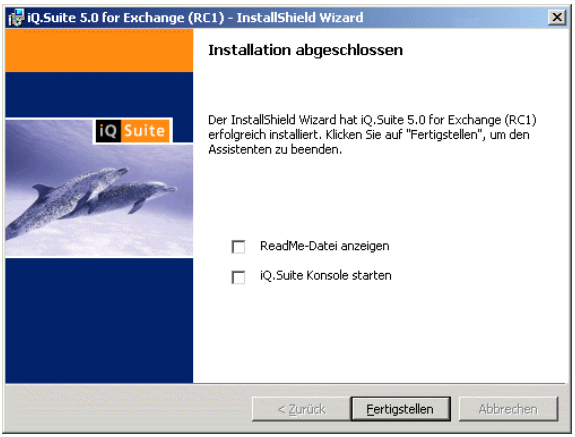


3. Damit das iQ.Suite Setup auf den passiven Knoten funktioniert, müssen alle Registry-Pfade der iQ.Suite auf gültige Verzeichnisse bzw. Dateien zeigen. Daher müssen ggf. in der Sektion **General** der iQ.Suite Registry-Einstellungen die Werte **Config**, **Data** und **InQ** geändert werden. In unserem Beispiel werden sie auf dem passiven Knoten CLNODE2 auf die Ursprungs-Verzeichnisse nach dem initialen iQ.Suite Setup gesetzt. Falls diese Verzeichnisse nicht mehr vorliegen, sollten sie „von Hand“ angelegt werden. Als **ConfigData.xml** kann diejenige des entsprechenden EVS kopiert werden:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
General]
"Data"="C:\GrpData\"
"Config"="C:\Program Files\GROUP Technologies\iQ.Suite\Config\
ConfigData.xml"
"InQ"="C:\GrpData\InQ"
```



4. Starten Sie das Setup der iQ.Suite für Exchange V5.0 auf dem passiven Knoten mit den entsprechenden Kommandozeilenparametern (siehe "Lokale Installation der iQ.Suite" auf Seite 39). Die weiteren Schritte des Updates der iQ.Suite sind die gleichen wie beim Update im NICHT-Cluster-Fall (siehe "Update von iQ.Suite 3.x oder 4 auf Version 5" auf Seite 26). Deaktivieren Sie am Ende des Updateprozesses die Option **Launch iQ.Suite Console**. Ansonsten wird ein Update der Konfigurationsdatei gemacht, was zu diesem Zeitpunkt unnötig ist.


iQ.Suite 5.0 for Exchange (RC1) - InstallShield Wizard
Installation abgeschlossen
iQ Suite
Der InstallShield Wizard hat iQ.Suite 5.0 for Exchange (RC1) erfolgreich installiert. Klicken Sie auf "Fertigstellen", um den Assistenten zu beenden.
ReadMe-Datei anzeigen
iQ.Suite Konsole starten
< Zurück
Fertigstellen
Abbrechen

5. Kopieren Sie eine gültige Lizenz-Datei in das Verzeichnis `…\iQ.Suite\License`.

5.6.2 Failover der EVS von CLNODE1 nach CLNODE2

Der momentane Stand der Installation sollte nun der Folgende sein: Auf allen passiven Knoten ist die iQ.Suite V5.0 installiert, auf allen aktiven Knoten läuft noch die „alte“ iQ.Suite V3.5 oder V4.0. Um auch die aktiven Knoten zu aktualisieren, müssen diese zu passiven Knoten gemacht werden. Dies wird durch den Failover der EVS erreicht. Dabei muss verhindert werden, dass durch die Registry-Replikation der iQ.Suite Cluster-Resource nach einem Failover eine iQ.Suite V5.0 mit alten Registry-Einträgen der V3.5 bzw. V4.0 läuft. Dies wird dadurch erreicht, dass die Registry-Replikation aus der iQ.Suite Cluster-Resource entfernt wird.

Damit der iQ.Suite Dienst auf dem vormals passiven Knoten nach dem Failover mit den korrekten Verzeichnissen auf der Disk-Resource arbeitet, müssen vor dem Failover „von Hand“ die Registry-Werte auf dem passiven Knoten auf die gleichen Werte wie die des aktiven Knotens gesetzt werden.

Außerdem sollte zur Sicherheit der SMTP-Dienst für die Dauer des Failovers deaktiviert werden. Nach erfolgreichem Failover kann dieser sofort wieder aktiviert werden.

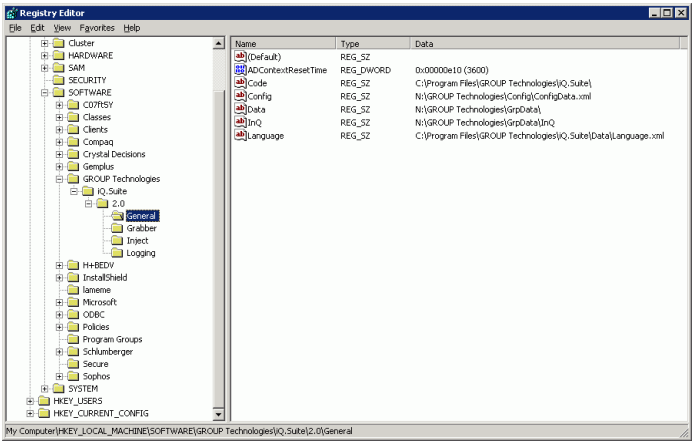
Im Folgenden werden die einzelnen Schritte anhand unseres Beispiels beschrieben:

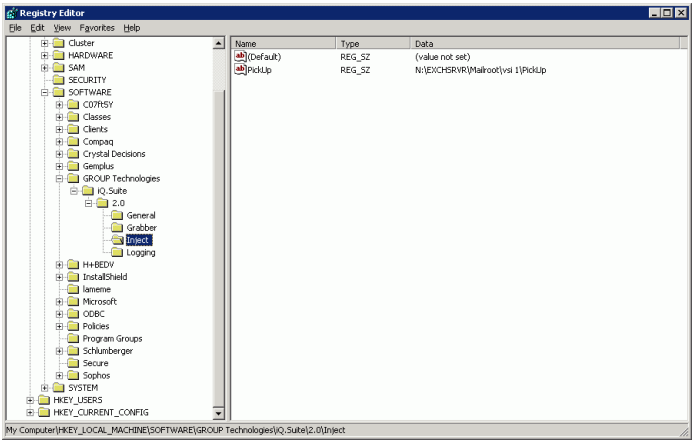
1. Anpassen der Registry auf dem passiven Knoten:
   Folgende Registry-Werte auf dem passiven Knoten müssen mit den korrespondierenden Registry-Werten auf dem aktiven Knoten abgeglichen werden:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
General]
"Data"
"Config"
"InQ"
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
Inject]
"PickUp"
```

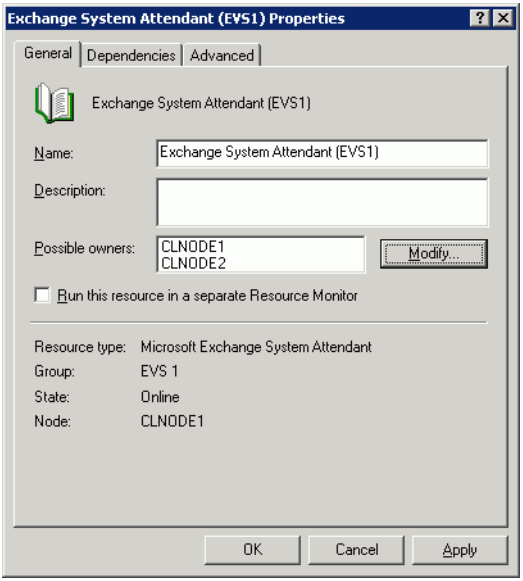
In unserem Beispiel bedeutet dies, dass die Werte wie folgt geändert werden:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
General]
"Data" = "N:\Group Technologies\GrpData"
"Config" = "N:\Group Technologies\config\ConfigData.xml"
"InQ" = "N:\Group Technologies\GrpData\InQ"
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
Inject]
"PickUp" = "N:\EXCHSRVR\MailRoot\vsi 1\PickUp"
```

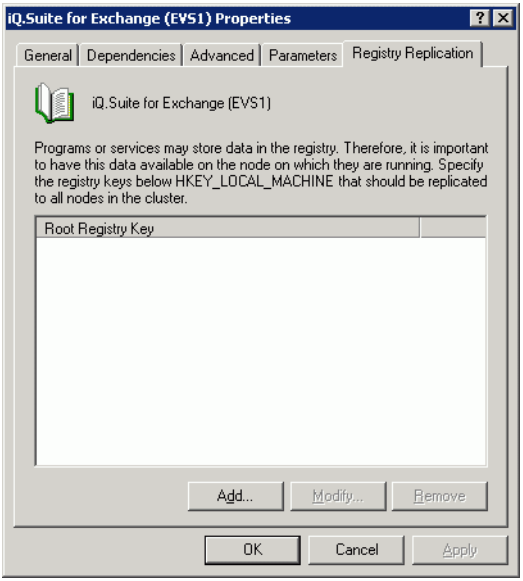




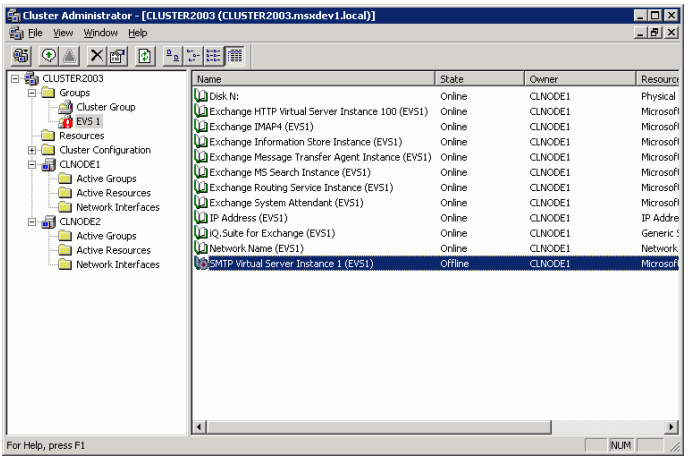
2. Öffnen Sie im Cluster Administrator über die rechte Maustaste die **Properties** der Resource **Exchange System Attendant**, wählen Sie die Registerkarte **General** und fügen Sie CLNODE2 in **Possible owners** hinzu (über **Modify...**), um ein Failover des EVS auf dem passiven Knoten wieder zu erlauben.



3. Öffnen Sie im Cluster-Administrator über die rechte Maustaste die **Properties** der iQ.Suite for Exchange-Resource, wählen Sie die Registerkarte **Registry Replication** und löschen Sie über **Remove** alle Einträge. Dadurch wird die Replikation der alten V3.5 Registry-Einträge auf dem aktualisierten passiven Knoten verhindert.


iQ.Suite for Exchange (EVS1) Properties
General
Dependencies
Advanced
Parameters
Registry Replication
iQ.Suite for Exchange (EVS1)
Programs or services may store data in the registry. Therefore, it is important to have this data available on the node on which they are running. Specify the registry keys below HKEY_LOCAL_MACHINE that should be replicated to all nodes in the cluster.
Root Registry Key
Add...
Modify...
Remove
OK
Cancel
Apply

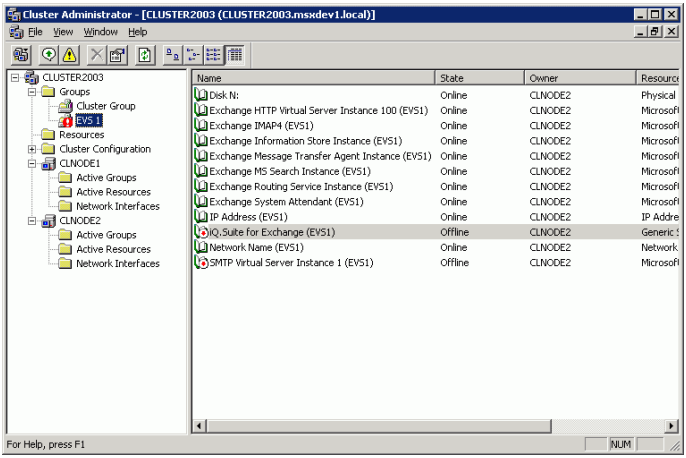
4. Setzen Sie den SMTP-Dienst im Cluster-Administrator offline: Klicken Sie mit der rechten Maustaste auf **SMTP Virtual Server Instance 1 (EVS1)** --> **Take offline**.



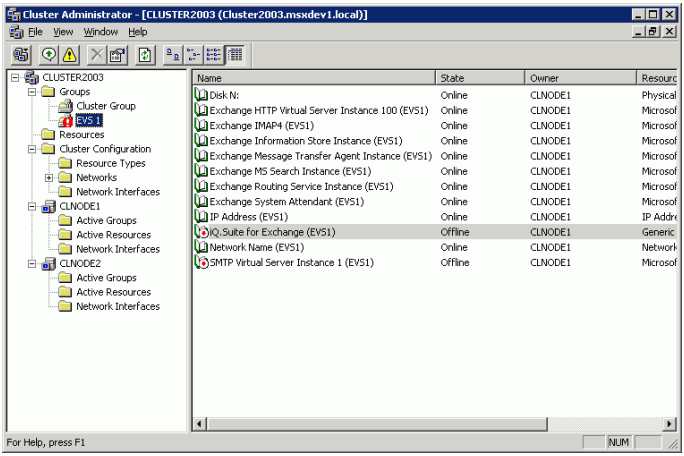
5. Warten Sie, bis die iQ.Suite Warteschlange leer ist. Diese befindet sich unter `N:\Group Technologies\GrpData\InQ` auf dem aktiven Knoten CLNODE1. Hier speichert die iQ.Suite temporär noch nicht bearbeitete

Mails. Erst wenn dieses Verzeichnis leer ist, kann der iQ.Suite Service offline genommen werden.

6. Setzen Sie die iQ.Suite Cluster-Resource offline (analog zu Punkt 4).



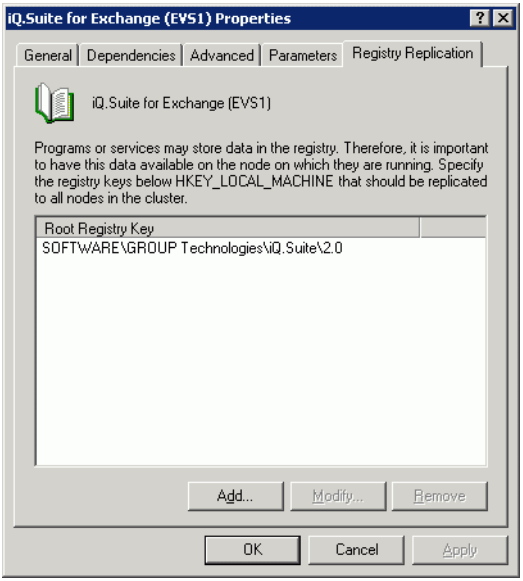
7. Failover auf passiven Knoten CLNODE2: Wählen Sie im Cluster-Administrator mit der rechten Maustaste **EVS 1** --> **Move Group**. Der Failover wird nun gestartet.
8. Nachdem der Failover erfolgreich abgeschlossen ist (siehe nächste Abbildung), starten Sie auf CLNODE2 (vormals passiver Knoten) die iQ.Suite Konsole (siehe “Die iQ.Suite Konsole” auf Seite 71 und “Starten der iQ.Suite Konsole” auf Seite 17). Es erscheint eine Dialogbox, die anzeigt, dass die Konfiguration aktualisiert wird. Bestätigen Sie die Meldung mit **OK**. Dadurch wird ein Update der Konfigurationsdatei (**ConfigData.xml**) auf der Disk-Resource `N:` gestartet. Dieser Vorgang kann einige Minuten dauern.



9. Setzen Sie die iQ.Suite Cluster-Resource über den Cluster Administrator online (rechte Maustaste auf **iQ.Suite for Exchange (EVS1)** und auf **Bring online** klicken). Überprüfen Sie anschließend im Event Log, ob die Konfigurationsdatei (**ConfigData.xml**) von `N:` geladen wurde und der Dienst ohne Warnungen oder Fehler gestartet wurde.
10. Aktivieren Sie nun wieder die Registry-Replikation der iQ.Suite Cluster-Resource: Öffnen Sie im Cluster-Administrator über die rechte Maustaste die **Properties** der iQ.Suite for Exchange-Resource, wählen Sie die Registerkarte **Registry Replication** und fügen Sie über die **Add…**-Schaltfläche den Registry Key

    `SOFTWARE\GROUP Technologies\iQ.Suite\2.0`

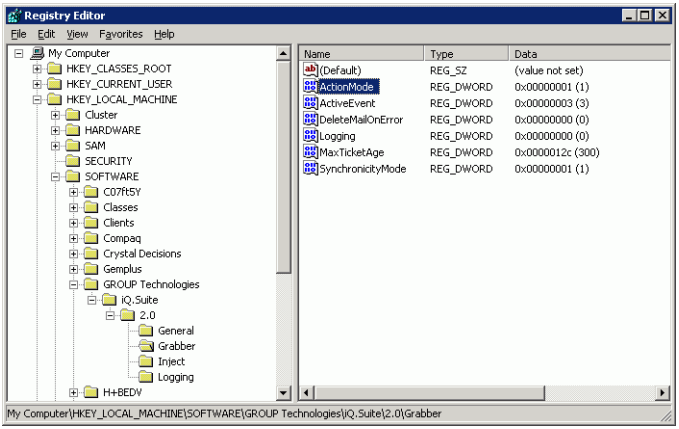
    hinzu. Schließen Sie den Dialog mit **OK**.


iQ.Suite for Exchange (EVS1) Properties
General
Dependencies
Advanced
Parameters
Registry Replication
iQ.Suite for Exchange (EVS1)
Programs or services may store data in the registry. Therefore, it is important to have this data available on the node on which they are running. Specify the registry keys below HKEY_LOCAL_MACHINE that should be replicated to all nodes in the cluster.
Root Registry Key
SOFTWARE\GROUP Technologies\iQ.Suite\2.0
Add...
Modify...
Remove
OK
Cancel
Apply

11. Aktivieren Sie auf CLNODE 2 den iQ.Suite Grabber. Dazu ändern Sie den Registry-Wert **ActionMode** in der Sektion **Grabber** der iQ.Suite Registry-Einstellungen von 0 auf 1.

Achtung: die Cluster-Resource **iQ.Suite for Exchange (EVS1) muss** während dieses Installationsschrittes auf CLNODE2 **Online** sein.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
Grabber]
"ActionMode"= dword:00000001
```



12. Setzen Sie den SMTP-Dienst im Cluster Administrator wieder online, indem Sie mit der rechten Maustaste auf **SMTP Virtual Server Instance 1 (EVS1)** klicken und dann **Bring online** wählen.

5.6.3 Update des vormals aktiven Knotens CLNODE1

Das Update erfolgt analog zu Abschnitt "Update der passiven Knoten CLNODE1" auf Seite 55. Nach dem Update tragen Sie diesen Knoten unter **Possible owners** der **Exchange System Attendant**-Ressourcen aller EVS im Cluster wieder ein.

5.6.4 Fallback auf Ursprungsknoten

Nach dem Update von CLNODE1 und CLNODE2 kann optional ein Fallback des EVS1 von CLNODE2 nach CLNODE1 erfolgen, um den Ursprungszustand des Clusters wiederherzustellen. Falls erwünscht, können Sie Schritt 1 aus Abschnitt "Update der passiven Knoten CLNODE1" auf Seite 55 wieder auf Ursprungswerte setzen.

5.6.5 Beispiel eines Updates auf einem 4-Knoten Cluster

Anhand des beschrieben Szenarios von "Beispiel einer Erstinstallation auf einem 4-Knoten-Cluster" auf Seite 50 und der obigen Update-Beschreibung werden hier die Update-Schritte auf 4-Knoten Clustern kurz beschrieben.

Zuerst wird der passive Knoten CLNODE4 aktualisiert und danach sukzessive die Knoten CLNODE1 – CLNODE3 per Failover nach CLNODE4 mit anschließendem Update.

- Update aller passiven Knoten:
  - Update des passiven Knotens CLNODE4 (Abschnitt "Update der passiven Knoten CLNODE1" auf Seite 55).
- Update CLNODE1
  - Failover EVS1 von CLNODE1 nach CLNODE4 (Abschnitt "Failover der EVS von CLNODE1 nach CLNODE2" auf Seite 58).
  - Update des passiven Knotens CLNODE1.
  - Fallback EVS1 von CLNODE4 nach CLNODE1 (Abschnitt "Fallback auf Ursprungsknoten" auf Seite 65).
- Update CLNODE2:
  - Failover EVS2 von CLNODE2 nach CLNODE4.
  - Update des passiven Knotens CLNODE2.
  - Fallback EVS2 von CLNODE4 nach CLNODE2.
- Update CLNODE 3:
  - Failover EVS3 von CLNODE3 nach CLNODE4.
  - Update des passiven Knoten CLNODE3.
  - Fallback EVS3 von CLNODE4 nach CLNODE3.

5.7 Deinstallation der iQ.Suite in einem Cluster

Die Deinstallation der iQ.Suite erfolgt in mehreren Schritten:

1. Deaktivieren des Grabbers (nur auf aktiven Knoten)
2. Warten, bis iQ.Suite Warteschlangen leer sind (nur auf aktiven Knoten)
3. Entfernen der iQ.Suite Cluster-Ressource im Cluster Administrator
4. Deinstallation auf allen Knoten
5. Löschen der iQ.Suite Verzeichnisse auf Disk-Resourcen

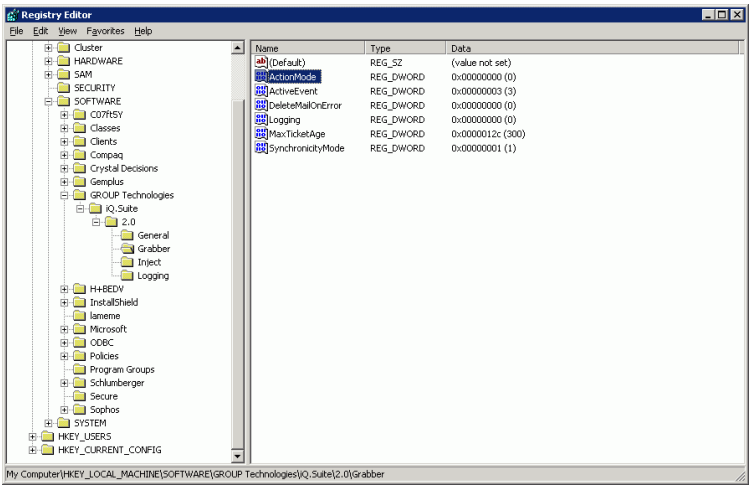
Im Folgenden werden die einzelnen Schritte beschrieben.

5.7.1 Deaktivieren des Grabbers

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

Ändern Sie den Registry-Wert **ActionMode** in der Sektion **Grabber** der iQ.Suite Registry-Einstellungen von 1 auf 0.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
Grabber]
"ActionMode"= dword:00000000
```



5.7.2 Warten, bis iQ.Suite Warteschlangen leer sind

Achtung: Dieser Schritt ist nur auf aktiven Knoten nötig!

Durch die Deaktivierung des Grabbers werden keine Mails mehr vom Exchange System in die iQ.Suite Warteschlangen gestellt. Allerdings können noch Mails in Bearbeitung sein. Warten Sie deshalb solange, bis das Verzeichnis **InQ** im **Grp-Data**-Verzeichnis auf der entsprechenden Disk-Resource der iQ.Suite Cluster-Resource leer ist und auch leer bleibt.

5.7.3 Entfernen der iQ.Suite Cluster-Resource

Entfernen Sie über den Cluster Administrator nun die iQ.Suite Cluster-Resource: Klicken Sie mit der rechten Maustaste auf **iQ.Suite Cluster-Resource** und dann auf **Delete**.

Führen Sie vorher für diese iQ.Suite Cluster-Resource unbedingt die Schritte aus Deaktivieren des Grabbers und Warten, bis iQ.Suite Warteschlangen leer sind aus!

5.7.4 Lokale Deinstallation auf allen Knoten

Sobald alle iQ.Suite Cluster-Ressourcen im Cluster entfernt worden sind, deinstallieren Sie die iQ.Suite auf jedem Knoten über den **Add/Remove Programs**-Dialog im **Control Panel**. Damit die Deinstallation auf den Knoten erfolgreich ausgeführt werden kann, müssen alle Registry-Pfade der iQ.Suite auf gültige Verzeichnisse bzw. Dateien zeigen. Ändern Sie daher ggf. in der Sektion **General** der iQ.Suite Registry-Einstellungen die Werte **Config**, **Data** und **InQ**. Auf allen aktiven Knoten sollten diese Pfade noch auf gültige Verzeichnisse auf der Disk-Resource zeigen, also z.B.:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technologies\iQ.Suite\2.0\
General]
"Data"="N:\GROUP Technologies\GrpData\"
"Config"="N:\GROUP Technologies \iQ.Suite\Config\ConfigData.xml"
"InQ"="N:\GROUP Technologies GrpData\InQ"
```

Sind diese Verzeichnisse noch gültig, kann die Deinstallation direkt gestartet werden.

Auf passiven Knoten dagegen können hier ungültige (also nicht existente) Pfade stehen. Um eine Deinstallation zu ermöglichen, können Sie entweder:

- ein Failover des entsprechenden EVS auf diesen Knoten machen, damit die Disk-Resource wieder erreichbar ist.
- die Verzeichnisse lokal „von Hand“ auf der Knoten anlegen und danach die Registry-Werte anpassen. Als **ConfigData.xml** kopieren Sie die des ent-

sprechenden EVS (siehe “Update der passiven Knoten CLNODE1” auf Seite 55 Schritt 3), z.B.:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GROUP Technolo-
gies\iQ.Suite\2.0\General]
"Data"="C:\GrpData\"
"Config"="C:\Program Files\GROUP Technologies\iQ.Suite\Con-
fig\ConfigData.xml"
"InQ"="C:\GrpData\InQ"
```

Danach ist die Deinstallation auch auf passiven Knoten möglich.

5.7.5 Löschen der iQ.Suite Verzeichnisse auf Disk-Resourcen

Abschließend löschen Sie die kopierten iQ.Suite Verzeichnisse auf den Disk-Resourcen.

6 Allgemeines

6.1 Die iQ.Suite Architektur

Die iQ.Suite für Exchange gliedert sich in drei Hauptbestandteile:

- Die iQ.Suite Konsole
- Der iQ.Suite Server
- Die iQ.Suite Konfiguration (siehe dazu auch "Konfiguration in der iQ.Suite Management Konsole" auf Seite 84).

6.1.1 Die iQ.Suite Konsole

Die iQ.Suite Konsole ist das „Cockpit", aus dem die iQ.Suite konfiguriert und administriert wird. Es handelt sich hierbei um ein sogenanntes „Snap-In" für die MMC (Microsoft Management Console). Mit der iQ.Suite Konsole können sowohl einzelne Exchange-Server mit installierter iQ.Suite administriert werden als auch ganze „iQ.Suite Serverfarmen". Dies erleichtert speziell in einer Multi-Server-Umgebung die tägliche Administration. Mit der iQ.Suite Konsole erhält der Administrator Zugriff auf alle erforderlichen Konfigurationsinformationen und den iQ.Suite Monitor (Quarantäne) der iQ.Suite Server.

Für die Konfiguration und die Zugriffe auf die Quarantänen werden zwei unterschiedliche Zugriffsmethoden verwendet.

1. Standard Windows Dateizugriff
   Für den Zugriff auf die iQ.Suite Konfiguration, um beispielsweise Sicherheitseinstellungen zu administrieren, ist ein Windows Dateizugriff erforderlich. Hierbei kann die iQ.Suite Konfiguration lokal zur Verfügung stehen oder über einen Universal Naming Convention (UNC) Pfad erreicht werden.

2. SOAP und SSL
   Der Zugriff auf den iQ.Suite Monitor (siehe "iQ.Suite Monitor" auf Seite 123) erfolgt über SOAP und SSL. Dabei wird über einen festgelegten Kommunikationsport kommuniziert.

Die iQ.Suite Konsole unterstützt zwei Betriebsmodi.

1. Lokale Administration

   Hierbei wird die iQ.Suite Konsole direkt auf dem Exchange-Server betrieben, auf welchem alle Komponenten der iQ.Suite installiert wurden. Dieser Modus eignet sich für kleinere Umgebungen und die Administration am Server vor Ort.

2. Remote Administration

   In diesem Fall wird die iQ.Suite Konsole nicht auf dem Exchange-Server, sondern auf einem Client installiert.

   Die iQ.Suite Konsole ist auf folgenden Client-Betriebsystemen lauffähig:

   - Windows 2000 Professional
   - Windows 2003
   - Windows XP Professional

Die Remote Administration eignet sich für die zentrale Administration in Multi-Server-Umgebungen. Die iQ.Suite Konsole greift dabei auf einen oder mehrere Exchange-Server zu, um die iQ.Suite zu konfigurieren und administrieren.

6.1.2 Der iQ.Suite Server

Mit iQ.Suite Server werden die Funktionen und Prozesse der iQ.Suite bezeichnet, die ausschließlich auf dem Exchange-Server laufen. Hierbei kann der iQ.Suite Server auf einem Exchange-Server, Front-End Server oder Back-End Server installiert werden. Der iQ.Suite Server unterteilt sich wiederum in verschiedene Bereiche.

6.1.2.1 Der Grabber

Der Grabber ist ein Prozess, der dafür zuständig ist, dass alle E-Mails, Terminanfragen, etc., die der Exchange Server versendet, empfängt oder routet, „abgegriffen“ (englisch: to grab) werden. Für den gesamten Transport von E-Mails, Terminanfragen, etc. wird das SMTP Transportprotokoll verwendet. Ein Bestandteil des SMTP Transportprotokolls ist der „SMTP Erweiterte Warteschlangen Mechanismus“ (englisch: „SMTP Advanced Queue“). Durch diese Advanced Queue wird der komplette E-Mail-Verkehr geleitet. Dabei ist es unerheblich, ob es

sich um E-Mails handelt, die zwischen Postfächern auf dem gleichen Postfachspeicher oder Server gesendet werden oder um ein- und ausgehende E-Mails.

In allen Fällen müssen E-Mails die Advanced Queue durchlaufen.

Der Grabber ist in diese Advanced Queue „eingeklinkt“. Als registrierte Ereignissenke (englisch: Event Sink) überwacht der Grabber dort den E-Mail-Verkehr und leitet alle relevanten Informationen an den iQ.Suite Service - die zweite Komponente des iQ.Suite Server - weiter. Die E-Mail wird so lange aufgehalten, bis die gesamte Verarbeitung durch den iQ.Suite Server erfolgreich beendet ist.

Exchange-interne Informationen, wie beispielsweise Replikationsnachrichten, werden vom Grabber als solche erkannt und unverändert an das Exchange-System zurückgegeben.

6.1.2.2 Der iQ.Suite Service = Enterprise Message Handler (EMH)

Der iQ.Suite Service ist als Windows Dienst permanent gestartet und übernimmt alle Informationen vom Grabber. Die gesamte Weiterverarbeitung durch die iQ.Suite wird ab diesem Zeitpunkt vom iQ.Suite Service überwacht und gesteuert. Der iQ.Suite Service hat Zugriff auf alle notwendigen Informationen. Dies sind beispielsweise:

- Die konfigurierten iQ.Suite Jobs
- Die installierte iQ.Suite Lizenz
- Das Active Directory
- Die iQ.Suite Quarantäne

Mit Hilfe all dieser Informationen werden die E-Mails nun beispielsweise nach Viren gescannt, Spam E-Mails identifiziert und in Quarantäne gestellt oder Haftungsausschlusserklärungen integriert.

Nach der Bearbeitung übergibt der iQ.Suite Service die E-Mails über das Pickup-Directory wieder an den Exchange-Server.

Sobald der iQ.Suite Grabber installiert ist, werden alle E-Mails in die iQ.Suite In-Queue[4] kopiert. Von dort aus sorgt der iQ.Suite Service für die Weiterverarbeitung. Ist der iQ.Suite Service nicht gestartet, werden die E-Mails inkl. der XML-

4. siehe “Die iQ.Suite In-Queue” auf Seite 77

Dateien in der iQ.Suite In-Queue so lange gespeichert, bis der iQ.Suite Service wieder gestartet ist und die Weiterverarbeitung fortgesetzt wird.

6.1.2.3 Die iQ.Suite Quarantäne

Als eine mögliche Option können virenverseuchte E-Mails oder andere unerwünschte E-Mails auf dem Server gestoppt werden. Damit wird verhindert, dass diese E-Mails bei den entsprechenden Empfängern ankommen. Diese E-Mails werden statt dessen in der iQ.Suite Quarantäne abgelegt. Auf jedem iQ.Suite Server stehen nach der Installation einige Quarantänen zur Verfügung. Weitere Quarantänen können vom Administrator angelegt werden.

Eine iQ.Suite Quarantäne besteht aus

- einem Quarantäneverzeichnis auf dem Exchange-Server (`..\Grp-Data\Quarantine\Standard-Quarantaene`),
- den E-Mails, die in die Quarantäne kopiert wurden,
- einer Quarantäne Datenbank (**LocIdxDB.mdb**).

Für jede in Quarantäne gestellte E-Mail erzeugt die iQ.Suite automatisch einen Eintrag in der Quarantänedatenbank. Bei dieser Datenbank handelt es sich um eine Microsoft Access Datei.

In dieser Datenbank werden folgende Informationen abgelegt:

- E-Mail Betreff
- Datum/Uhrzeit
- E-Mail Sender
- E-Mail Empfänger
- Kurzbeschreibung der entdeckten Restriktion
- E-Mail-Größe
- Name des iQ.Suite Jobs, der diese E-Mail in Quarantäne stellte
- Name des Exchange-Servers
- Name der Maildatei
- Bearbeitungshistorie

Beim Anzeigen einer iQ.Suite Quarantäne mit der iQ.Suite Konsole werden zunächst die Informationen aus der Quarantänedatenbank angezeigt. Beim Öffnen eines Quarantäneeintrags werden weitere Informationen aus der Maildatei geladen.

Der Kommunikation mit der iQ.Suite Quarantäne erfolgt mit Hilfe von SOAP (Simple Object Access Protocol) + SSL (Secure Socket Layer). Dies gilt sowohl für den „lokalen“ Zugriff auf dem Server direkt als auch für den Zugriff von einer entfernten Windows Workstation. Dabei wird für die Kommunikation standardmäßig der Port 8008 verwendet. Dieser Port kann in der iQ.Suite Konsole (Knoten „**iQ.Suite Servers**“) verändert werden. Wird dieser Port für den Server verändert, so muss diese Änderung auch auf allen zugreifenden iQ.Suite Konsolen angepasst werden. Alle Rechner müssen den gleichen Port verwenden. Mit Hilfe von SSL wird der SOAP Kommunikationskanal verschlüsselt. Während der Installation werden hierfür alle notwendigen Komponenten bereitgestellt.

Auf die iQ.Suite Quarantänen können nur autorisierte Personen zugreifen. Die Benutzerberechtigungen werden über die Eigenschaften der Datei **access.acl** (`..\GROUP Technologies\iQ.Suite\AppData\`) vergeben. Diese Berechtigungen werden durch den iQ.Suite Service geprüft. Sie müssen sich beim **ersten** Aufruf der Quarantänen authentifizieren. Danach werden die Authentifizierungsinformationen zwischengespeichert, so dass bei weiteren Zugriffen (insbesondere auf andere Quarantänen) der Aufruf mit den vorher erfolgreichen Anmeldedaten erfolgt. Schlägt dies fehl, erscheint ein Dialog zur Eingabe von Benutzernamen und Passwort.

Für den erfolgreichen Zugriff müssen folgende Bedingungen erfüllt sein:

- Der iQ.Suite Service läuft
- Der Kommunikations Port (Standard:8008) ist verfügbar
- Der Rechnername ist auflösbar und über TCP/IP erreichbar
- Der Benutzer besitzt die erforderlichen Windows-Benutzerberechtigungen

6.1.2.4 Das Active Directory / LDIF

Die iQ.Suite nimmt keine Veränderungen oder Erweiterungen im Active Directory vor. Informationen aus dem Active Directory werden jedoch an verschiedenen Stellen von der iQ.Suite ausgelesen.

Beim Starten ermittelt der iQ.Suite Service den verfügbaren Global Catalog Server. Dieser wird zum Beispiel bei der Adressauflösung von Verteilerlisten während der E-Mail-Verarbeitung verwendet.

Die iQ.Suite Konsole verwendet das Active Directory bei der Auswahl von Sender/Empfänger Bedingungen.

Mit iQ.Suite Trailer können Absenderinformationen in ausgehende E-Mails integriert werden. Dabei sucht die iQ.Suite im Active Directory nach den entsprechenden Angaben.

Steht kein Active Directory zur Verfügung, da z. B. die entsprechenden Ports nicht offen sind, kann mit einer LDIF-Datei gearbeitet werden. Diese kann beispielsweise durch einen LDAP Export aus einem Active Directory, Exchange 5.5 Benutzerverzeichnis oder einem Notes Names- und Adressbuch (NAB) erzeugt werden.

6.1.2.5 Die Windows Registry

Bei der Installation der iQ.Suite werden einige Registryschlüssel erstellt. Diese Einträge verwendet sowohl der iQ.Suite Server als auch die iQ.Suite Konsole.

Die Schlüssel befinden sich unter

```
HKEY_LOCAL_MASCHINE\SOFTWARE\GROUP TECHNOLOGIES\iQ.Suite
```

Darunter existieren weitere Schlüssel

- General (z.B. Standardpfade)
- Grabber (Konfiguration der iQ.Suite Event Sinks in der SMTP Advanced Queue)
- Inject (Pfad zum Exchange Pickup Verzeichnis)
- Logging (Debuglog Einstellungen)

6.1.2.6 Komprimierte Dateien/Archive: Der iQ.Suite Entpacker

Wenn Dateien per E-Mail verschickt werden, geschieht das häufig in komprimierter Form. Damit der Virenscan und alle Prüfungen auch bei Archiven funktionieren, benutzt die iQ.Suite einen Entpacker, um Dateien innerhalb der Archive prüfen zu können. Die iQ.Suite beinhaltet einen Entpacker, der mit der Installation automatisch zur Verfügung steht.

Der Entpacker unterstützt die folgenden Archivformate:

- ACE
- CAB

- ZIP
- Selfextracting ZIP
- ARJ
- Selfextracting ARJ
- TAR
- GZIP
- TGZ (Tape Archiv)
- UUE (Executable compressed ASCII archive)
- LZH (LH ARC)
- RAR
- Selfextracting RAR
- Java Archive (.jar)
- BZIP2

Innerhalb eines Archivs können sich wiederum Archive befinden. Diese Archive (rekursiv gepackte Dateien) werden standardmäßig bis zu einer Entpackungstiefe von 5 entpackt. Alle Archive, die dieses Limit überschreiten, werden in den Bad-Mail-Bereich (siehe "Bad-Mails" auf Seite 132) überführt.

Die Standard-Obergrenze für entpackte Dateien beträgt 500 MB. Insbesondere bei sogenannten „ZIPof Death"-Attacken ist eine solche Limitierung wichtig.

Die Entpackungstiefe und die Platzlimitierung können in der Konsole unter **iQ.Suite Servers --> Eigenschaften -->** Registerkarte **Allgemeines** geändert werden.

6.1.2.7 Die iQ.Suite In-Queue

Der iQ.Suite Grabber kopiert alle zu verarbeitenden E-Mails in die iQ.Suite In-Queue. Diese befindet sich im Verzeichnis `..\Grpdata\InQ`. In diesem Verzeichnis befinden sich die E-Mails zunächst in der Originalform. Zusätzlich zu jeder E-Mail erstellt der Grabber eine dazugehörige XML Datei. Diese Datei enthält beispielsweise Informationen aus dem SMTP Header.

Ein solches „Dateipaar“:

- **2C4A14A23BD144B3ACE09E6BE2D49603000.txt**
  (Enthält die original E-Mail)
- **2C4A14A23BD144B3ACE09E6BE2D49603000.xml**
  (Enthält die Zusatzinformationen)

6.1.3 Die iQ.Suite Konfiguration

Alle Informationen, die zum Betreiben der iQ.Suite erforderlich sind, werden in der iQ.Suite Konfiguration gespeichert. Die iQ.Suite Konfiguration liegt in Form einer XML-Datei (**ConfigData.xml**) vor.

Die **ConfigData.xml** ist ähnlich einer Datenbank angelegt. Für jeden Konfigurationsbereich sind verschiedene Einträge vorhanden. Da es sich bei der Konfiguration um eine einzelne Datei handelt, ist es sehr einfach, die Konfiguration zu verteilen und zu sichern. Für die Unterstützung bei Konfigurationsproblemen kann die **ConfigData.xml** an das GROUP Support Team gesendet werden, um die Konfigurationseinstellungen zu untersuchen.

Die Konfigurationsinformationen benötigt sowohl der iQ.Suite Server als auch die iQ.Suite Konsole. Der iQ.Suite Server erhält daraus z.B. die Daten über die auszuführenden iQ.Suite Jobs. Um mit der iQ.Suite Konsole Veränderungen in der Konfiguration vornehmen zu können, benötigt auch diese Zugriff auf die **ConfigData.xml**. Die iQ.Suite Konfiguration kann sowohl in einem lokalen Verzeichnis als auch auf einem Netzwerkshare gespeichert werden. Welche iQ.Suite Konfiguration die iQ.Suite Konsole bzw. der iQ.Suite Server verwendet, wird durch einen Eintrag in der Registry festgelegt. Der Pfad zur iQ.Suite Konfiguration kann im Format `C:\.....` oder als UNC Pfad (`\\Servername\Share\ConfigData.xml`) angegeben werden. Falls die angegebene iQ.Suite Konfiguration nicht verfügbar ist, verwendet die iQ.Suite die sogenannte „Last-Known-Good“-Konfiguration. Dies wird in der Windows Ereignisanzeige protokolliert. Die „Last-Known-Good“-Konfiguration ist pro Server lokal gespeichert und wird immer dann aktualisiert, wenn Veränderungen an der iQ.Suite Konfiguration vorgenommen wurden und der Zugriff von der iQ.Suite Konfiguration auf die „Last-Known-Good“- Konfiguration möglich ist.

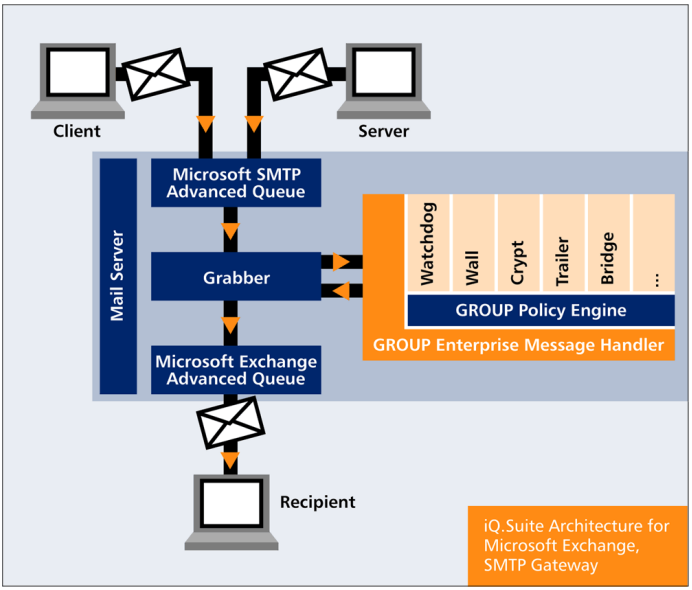
Um eine vom Standard abweichende Konfiguration mit der Konsole öffnen zu können, steht ein Parameter zur Verfügung. Starten Sie die **GROUP.msc** Datei mit dem Parameter **config** und der gewünschten Konfigurationsdatei, beispielsweise so:

```
"C:\Programme\GROUP Technologies\iQ.Suite\GROUP.msc" config "C:\AndererOrdner\verzeichnis\ConfigData.xml"
```

Sie können auch hier einen UNC-Pfad angeben.

Eine genaue Anleitung für die Einrichtung der iQ.Suite Konfiguration finden Sie in “Konfiguration in der iQ.Suite Management Konsole” auf Seite 84.

6.2 Ablauf der E-Mail-Verarbeitung



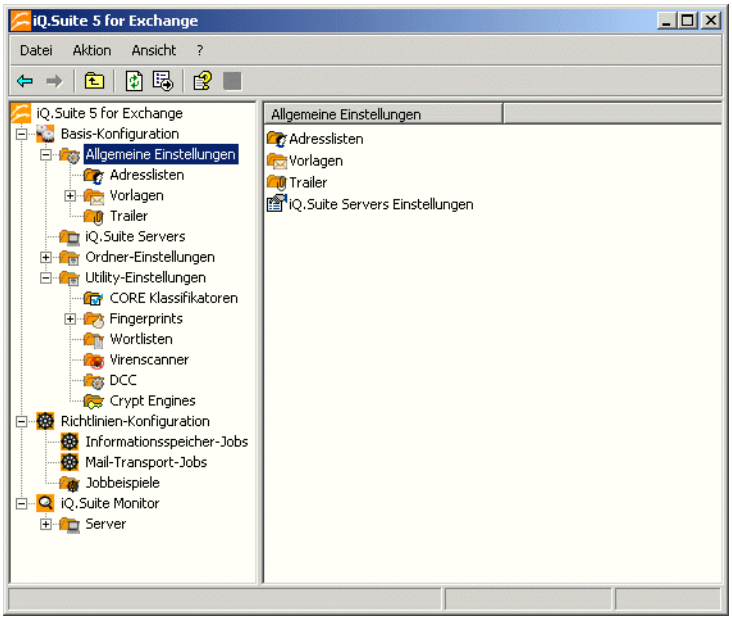
Es gilt folgender Ablauf:

1. Eine E-Mail trifft auf dem Mail-Server ein.
2. Die E-Mail wird durch den Grabber aus der SMTP Advanced Queue abgefangen und in einen speziellen Ordner gestellt.

3. Der Enterprise Message Handler (EMH) [= iQ.Suite Service] holt sich die E-Mail aus dem Ordner.
4. Der EMH überprüft anhand der Konfiguration, ob die E-Mail durch die iQ.Suite zu bearbeiten ist. Ansonsten wird die Mail sofort wieder der SMTP Advanced Queue zugeführt.
5. Zu bearbeitende Mails werden gemäß der Konfiguration (Jobs nach ihrer Priorität) abgearbeitet.
6. Der EMH gibt nach vollständiger Bearbeitung die E-Mail frei und stellt die Mail dem Exchange-Server zur Verfügung.

6.3 Die Benutzeroberfläche

Nach dem Öffnen der iQ.Suite wählen Sie in der linken Spalte die **Basis**-, die **Richtlinien-Konfiguration** oder **iQ.Suite Monitor**. Im rechten Fenster erscheinen die entsprechenden Unterordner. Klicken Sie für den Aufruf der Online-Hilfe oben in der Symbolleiste auf oder im Menü **Vorgang** auf **Hilfedatei anzeigen**.



6.3.1 Die Symbolleiste:

	Menü
	Ansichteinstellungen
	Zurück
	Vorwärts
	Eine Ebene höher
	Linke Spalte anzeigen/verbergen
	Eigenschaften des ausgewählten Objekts
	Ansicht aktualisieren
	Exportliste
	Hilfe
	Speichern
	Priorität um eins hochsetzen
	Priorität um eins runtersetzen
	Job aktivieren
	Job deaktivieren
	Neues Objekt
	Filter in Quarantäne/Badmail setzen
	Filter in Quarantäne/Badmail ausschalten

6.3.2 Bedeutung der Icons

	iQ.Suite Konsole Einstieg und Logo.
	Basis-Konfiguration für die allgemeinen Einstellungen aller Module.
	Knoten für **Allgemeine Einstellungen**.
	Der Ordner für die **Adresslisten**.

Eine einzelne **iQ.Suite Adressliste** (Kragen orange). die mit der iQ.Suite ausgeliefert wird und nicht geändert werden kann.

Eine einzelne **eigene Adressliste** (Kragen gelb), selbst anlegbar und unter **Eigenschaften** konfigurierbar.

Der Ordner für **Benachrichtigungsvorlagen**, der die einzelnen Vorlagen für jeden Jobtyp und Empfänger enthält.

Eine einzelne **Benachrichtigungsvorlage**, unter **Eigenschaften** konfigurierbar.

Der Ordner für die einzelnen **Trailer**, die als Übersicht in einer Liste gezeigt werden.

Das Symbol für einen einzelnen **Trailer**, unter **Eigenschaften** konfigurierbar.

Eine Liste aller iQ.Suite Server. Es lassen sich Server hinzufügen, entfernen und konfigurieren. Die gemeinsamen Eigenschaften aller Server werden unter **Allgemeine Einstellungen --> iQ.Suite Servers-Einstellungen** konfiguriert, alternativ mit der rechten Maustaste auf **iQ.Suite Servers --> Eigenschaften.** Dazu gehören die Standard-E-Mail-Adressen und die interne/n Domäne/n. Der Eintrag

Allgemeine **iQ.Suite Servers Einstellungen** unter dem Knoten **Allgemeine Einstellungen** im rechten Fenster.

Ein einzelner Server, unter **Eigenschaften** konfigurierbar.

Ordner-Einstellungen und **Utility-Einstellungen**. Unter Ordner-Einstellungen finden Sie die **Quarantänen** und **Bridge**, unter Utility-Einstellungen befinden sich alle zu konfigurierenden Zusätze wie **Virenscanner**, **CORE Klassifikatoren** oder **Crypt Engines**.

Die **Quarantäne-Ordner**struktur. Darunter befinden sich alle Quarantäne-Ordner.

Ein einzelner Quarantäne-Ordner, unter **Eigenschaften** konfigurierbar.

Die **Bridge** Quarantänenstruktur. Darunter befinden sich alle Bridge Quarantänen.

Eine einzelne **Bridge** Quarantäne, unter **Eigenschaften** konfigurierbar.

Ordner für **CORE Klassifikatoren**.

Ein einzelner **CORE Klassifikator**.

CORE Kategorien.

Der Ordner für **Fingerprint-Gruppen**.

Eine logisch zusammengehörende **Fingerprint-Gruppe**.

Ein einzelner **Fingerprint**, unter **Eigenschaften** konfigurierbar.

Der Ordner für die **Wortlisten**, mit denen die Inhaltsprüfung durchgeführt wird.

Eine einzelne **Wortliste**, unter **Eigenschaften** konfigurierbar.

Der Ordner für **Virenscanner-Anwendungen**.

Eine einzelne Virenscanner-Anwendung, unter **Eigenschaften** konfigurierbar.

Eine einzelne **DCC** Konfiguration.

Der Ordner für die einzelnen **Crypt Engines** (Verschlüsselungsanwendungen).

Eine einzelne **Crypt Engine**, unter **Eigenschaften** konfigurierbar.

Richtlinien-Konfiguration für die Konfiguration von individuellen Jobs nach den eigenen Firmenrichtlinien.

Ordner für **Jobbeispiele**, der die Jobs für die einzelnen Jobtypen enthält.

Ein Watchdog-Job, von dem es vier verschiedene Jobtypen gibt, unter **Eigenschaften** konfigurierbar.

Ein iQ.Suite Wall-Job, von dem es drei verschiedene Jobtypen gibt, unter **Eigenschaften** konfigurierbar.

Ein Crypt-Job, von dem es einen Jobtyp gibt, unter **Eigenschaften** konfigurierbar.

Ein Trailer-Job, von dem es einen Jobtyp gibt, unter **Eigenschaften** konfigurierbar.

Der **iQ.Suite Monitor** zur Einsicht in alle Quarantäne-Ordner auf jedem verfügbaren Server. Die Quarantäne-Ordner enthalten die Kopien der Original-E-Mails inklusive der Anhänge.

Die **Quarantäne**-Ordner mit Originalmails zur Einsicht. Für jede Mail können detaillierte Informationen abgerufen werden.

Ein einzelnes Quarantäneobjekt.

Ungültiges Quarantäneobjekt.

Erneut gesendetes Quarantäneobjekt.

Informationsspeicher-Quarantäneobjekt.

Uhrzeit und Wochentag einer **Quarantänewartung**.

Ordner für verschiedene, mit der iQ.Suite ausgelieferte **iQ.Suite Reports**.

Einzelner **iQ.Suite Report**.

6.4 Konfiguration in der iQ.Suite Management Konsole

Die Ansicht der iQ.Suite Konsole besteht aus drei Bereichen:

- Basis-Konfiguration
- Richtlinien-Konfiguration
- iQ.Suite Monitor

In der Basis-Konfiguration nehmen Sie allgemeine Einstellungen vor. Die **Basis-Konfiguration** rufen Sie im Regelfall nur einmal nach der Installation auf, um die wesentlichen Grundeinstellungen für alle Module durchzuführen. In der **Richtlinien-Konfiguration** setzen Sie die Firmenrichtlinien um, legen Jobs an und verwalten sie. Mit dem **iQ.Suite Monitor** können Sie die Quarantäne-Bereiche auf

jedem verfügbaren Server einsehen und erhalten detaillierte Informationen über die dort enthaltenen Mails.

6.5 Basis-Konfiguration

In der Basis-Konfiguration verwalten Sie die allgemeinen Einstellungen wie **Adresslisten**, die Benachrichtigungsvorlagen (**Vorlagen**) und **Trailer**, die **iQ.Suite Servers**, alle **Ordner** (z.B. die **Quarantänen**) und die Utilities: **CORE Klassifikatoren**, **Wortlisten** und den **DCC** Server für die Inhaltsprüfung, **Fingerprints** für das Blocken von Anhängen, die **Crypt Engines** für die Verschlüsselung und das Signieren und die **Virenscanner**.

6.5.1 Konfiguration importieren

Alle oben genannten Elemente/Objekte wie beispielsweise Wortlisten oder Fingerprints können unter **Basis-Konfiguration --> Alle Tasks --> Konfiguration importieren** neu eingespielt werden, wenn eine neue Version als Update verfügbar ist. Dazu wird die entsprechende XML-Datei ausgewählt, die GROUP zur Verfügung stellt.

Diese Funktion importiert nicht die vollständige Konfiguration (**ConfigData.xml**) inklusive der Jobs, sondern nur einzelne Basis-Objekte!

Bevor Sie ein Update eines Objektes der Basis-Konfiguration durchführen, empfiehlt es sich, eine Kopie des alten gleichnamigen Objekts zu erstellen und umzubenennen. Die neue Version ersetzt die alte, so dass anschließend Ihre eigenen Änderungen des Objektes verloren sind!

6.5.2 iQ.Suite Servers-Einstellungen

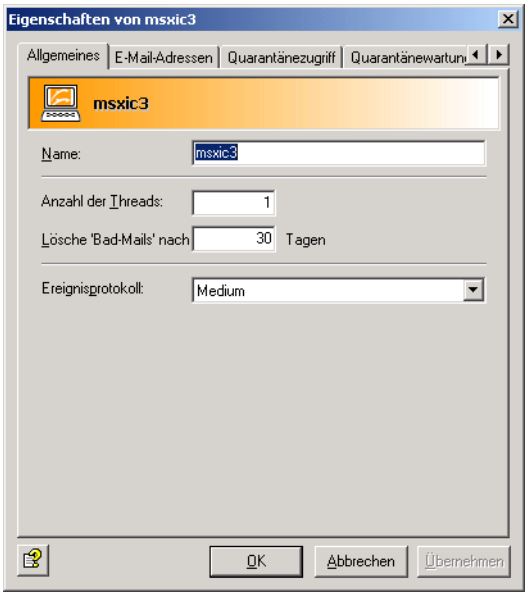
Die Konfiguration der übergreifenden Einstellungen für alle iQ.Suite Server finden Sie im Kapitel “Einstellungen von iQ.Suite Servers” auf Seite 20 und Hintergrundinformationen unter “Der iQ.Suite Server” auf Seite 72.

6.5.3 Einstellungen für einen einzelnen iQ.Suite Server

Wählen Sie **Basis-Konfiguration**, klicken Sie im linken Fenster auf **iQ.Suite Servers** und wählen Sie den gewünschten Server im rechten Fenster mit einem Doppelklick aus. Einen neuen Server erstellen Sie mit der rechten Maustaste auf

iQ.Suite Servers --> Neu --> iQ.Suite Server. Klicken Sie mit der rechten Maustaste auf **Eigenschaften**.

6.5.3.1 Allgemeine Servereinstellungen

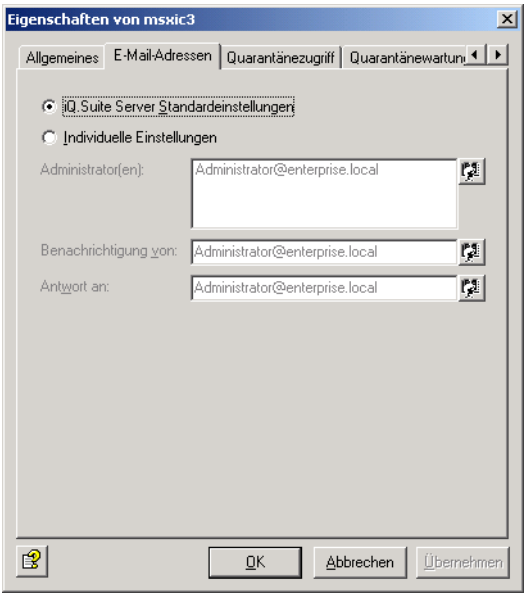


1. Tragen Sie den Namen des Exchange-Servers ein. Während der Installation wird der aktuelle Exchange-Servername automatisch eingetragen.
2. Bestimmen Sie die maximale Anzahl der gleichzeitig bearbeiteten E-Mails im Feld **Anzahl der Threads**. Die Standardeinstellung ist 1. Wie viele Mails sie gleichzeitig durch die iQ.Suite bearbeiten lassen können, hängt von der Ausstattung und Performance Ihres Servers ab.
3. Bestimmen Sie die Anzahl der Tage, die die Mails im Badmail-Bereich verbleiben sollen. Nach Ablauf dieser Tage werden die Mails automatisch gelöscht.
4. Wählen Sie die Protokollstufe für das **Ereignisprotokoll**, welches Sie mit dem Event Viewer/Ereignisanzeige einsehen können (Windows Event Log). Die Abstufungen reichen von **Kein Protokoll** bis **Maximum**.

Um auf den neuen Server sofort zugreifen zu können, aktualisieren Sie die Ansicht im Monitor (Rechte Maustaste auf **iQ.Suite Monitor -> Aktualisieren**).

6.5.3.2 Individuelle E-Mail-Adressen für einen iQ.Suite Server

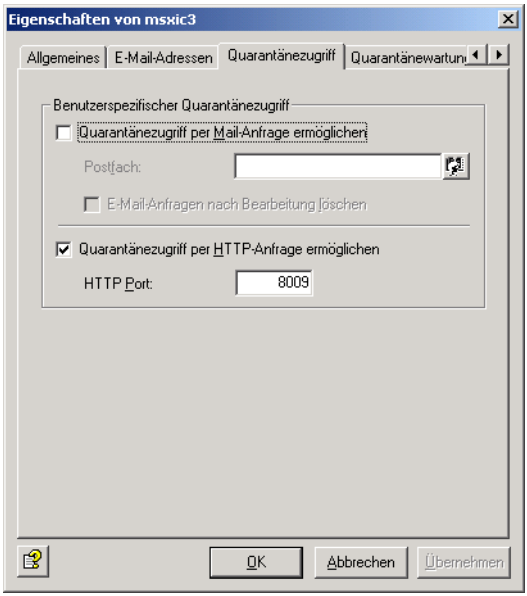
Für jeden einzelnen Server werden die Einstellungen aus den Eigenschaften aller **iQ.Suite Servers** übernommen, die während der Installation automatisch gesetzt werden oder von Ihnen individuell eingetragen worden sind. Diese Einstellungen gelten als **iQ.Suite Server Standardeinstellungen**. Sollten Sie für einen speziellen Server individuelle Einstellungen benötigen, aktivieren Sie die Option **Individuelle Einstellungen** und tragen Sie die Adressen in die entsprechenden Felder ein.



6.5.3.3 Benutzerspezifischer Zugriff auf die Quarantäne

Mit der iQ.Suite kann der Anwender selbst auf seine Quarantäne-Mails zugreifen. Welche Mails das sein sollen und welche Benutzer zugreifen dürfen, kann individuell für jede Quarantäne konfiguriert werden. Besonders interessant ist diese Funktion bei der Spam-Prüfung, also für die Spam-Quarantänen. Zusätzlich wird

der Administrator entlastet, da sich die Benutzer die einzelnen Quarantäne-Mails selbst zustellen können. Sie können für jeden Server definieren, ob und auf welche Art ein Anwender auf seine Quarantäne-Mails zugreifen darf. Der Anwender wird durch eine Sammelbenachrichtigung über die Quarantäne-Mails informiert, klickt auf die entsprechende Aktion für die gewünschte Mail und stellt damit eine Anfrage. Diese Aktion kann je nach Konfiguration **Anfordern**, **Freigeben** und/oder **Entfernen** sein. Der Zugriff durch den Anwender erfolgt über eine Mail-Anfrage oder über eine HTTP-Anfrage. Klicken Sie auf die Registerkarte **Quarantänezugriff**:



Quarantänezugriff per Mail-Anfrage ermöglichen: Die Anfrage an die Quarantäne(n) wird über eine Mail-Anfrage gestartet. Diese E-Mail wird automatisch erzeugt, wenn der Anwender in seiner Sammelbenachrichtigung auf den Aktionslink für die gewünschte Mail klickt[5] und an eine E-Mail- Adresse gesendet, die Sie auf dieser Registerkarte im Feld **Postfach** definieren. Voraussetzung ist, dass die hier angegebene E-Mail-Adresse existiert und dass die Mail über den Server gesendet wird, auf dem die iQ.Suite (und die entsprechenden Quarantäne(n)!)

5. siehe hierzu auch "Quarantäne-Sammelbenachrichtigungen einrichten" auf Seite 111

installiert ist. Wir empfehlen, das Postfach auf dem jeweiligen Server anzulegen. Der Inhalt der Mail wird ausgelesen und dadurch die vom Anwender gewünschte Aktion durchgeführt. Die iQ.Suite erkennt Anfrage-Mails der Anwender durch

1. die E-Mail-Adresse (Angabe im Feld **Postfach**)
2. das Schlüsselwort für eine Benutzeranfrage in der Mail (User Request)

Letztlich wird die Anforderungsmail im angegebenen Postfach abgelegt. Setzen Sie den Haken bei der Option **E-Mail-Anfragen nach Bearbeitung löschen**, wenn die Anfrage-Mails nach Abarbeitung aus dem angegebenen Postfach gelöscht werden sollen.

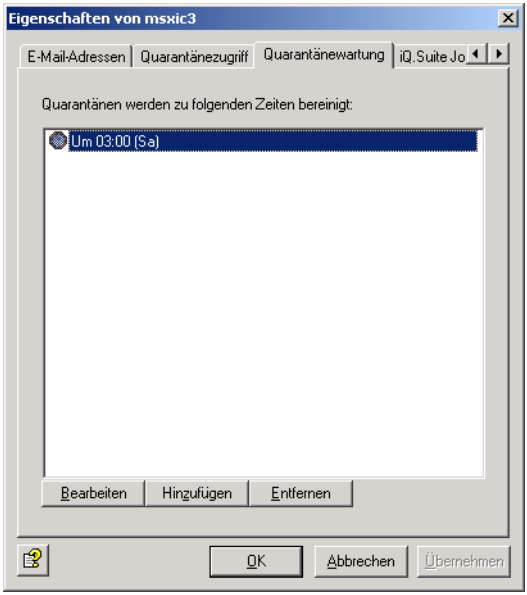
Quarantänezugriff per HTTP-Anfrage ermöglichen: Die Anfrage an die Quarantäne wird über HTTP gestartet. Sobald der Benutzer auf die gewünschte Aktion geklickt hat, öffnet sich der Standardbrowser. Der Benutzer erhält eine Meldung, dass seine Anfrage bearbeitet wird. Voraussetzung für diese Anfrage ist ein freier Port. Der Standardeintrag ist der Port 8009.

Achtung: Die Rückmeldung für den Anwender, die durch den Browser angezeigt wird, ist immer gleichlautend (OK_Response.html im Verzeichnis `iQ.Suite\AppData`). Sollte die angeforderte Mail also nicht mehr existieren, da sie beispielsweise in der Quarantäne bereits gelöscht wurde, so erhält der Benutzer darüber keinerlei Benachrichtigung.

Näheres über die Konfiguration des benutzerspezifischen Quarantänezugriffs finden Sie in “Quarantäne konfigurieren” auf Seite 110.

6.5.3.4 Quarantänewartung

Legen Sie hier den Zeitpunkt fest, zu dem die Quarantänen des Servers bereinigt werden sollen. Durch die Bereinigung werden alle zum Löschen markierten E-Mails in allen Quarantänen physisch gelöscht und der entsprechende Platz wieder freigegeben. Die Standardeinstellung für die Bereinigung ist jeden Samstag um 3 Uhr nachts.



Sie können eine Quarantäne bei Bedarf auch manuell bereinigen, indem Sie auf der entsprechenden Quarantäne im **iQ.Suite Monitor** mit der rechten Maustaste den Befehl **Alle Tasks --> Quarantäne bereinigen** wählen.

6.5.3.5 Liste aller Jobs ansehen

In der Registerkarte **iQ.Suite Jobs** erhalten Sie eine Liste aller Jobs, die auf diesem Server definiert sind.

Wenn Sie einen Job auf dem Server bearbeiten wollen, rufen Sie dazu direkt die Job-Eigenschaften auf. Siehe hierzu “Richtlinien-Konfiguration” auf Seite 118

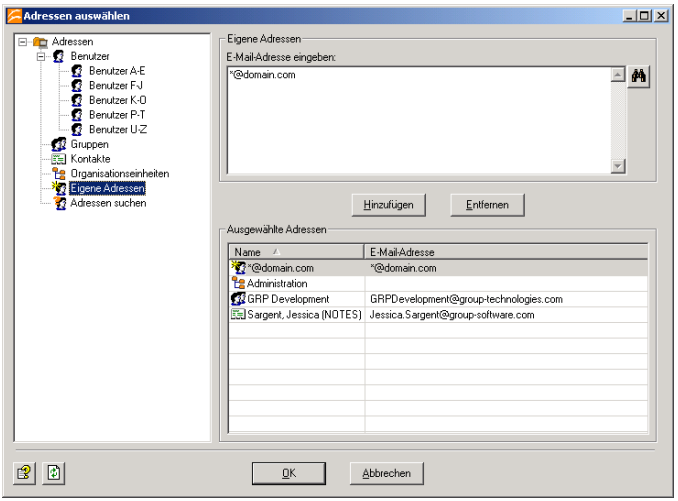
6.5.4 Adresslisten

6.5.4.1 Eigene Adresslisten anlegen, bearbeiten und löschen

In der **Basis-Konfiguration --> Allgemeine Einstellungen** unter **Adresslisten** können Sie eigene Adresslisten anlegen, die Sie im Job auswählen. Die zur Verfügung stehenden Adressen werden dem Active Directory entnommen.

Um eine Adressliste anzulegen, führen Sie folgende Schritte durch:

1. Klicken Sie auf **Adresslisten**.
2. Wählen Sie mit der rechten Maustaste den Eintrag **Neu --> Adressliste**.
3. Geben Sie der Adressliste einen sprechenden Namen.
4. Klicken Sie auf das Symbol für **Adressen auswählen**: .
5. Im folgenden Fenster wählen Sie aus den einzelnen Rubriken die gewünschten Adressen mit **Hinzufügen** aus:



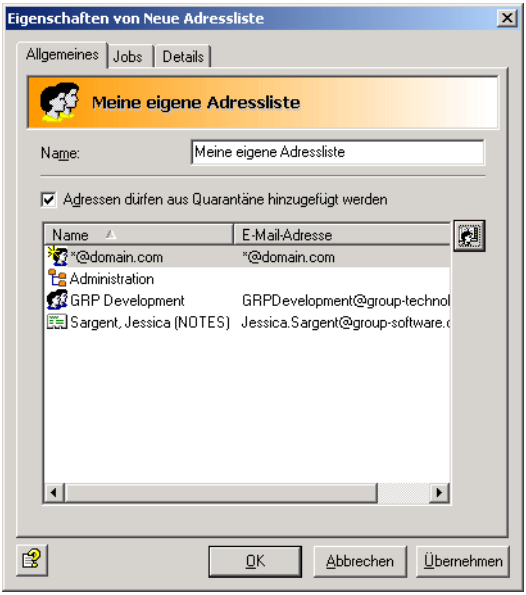
Eigene Adressen können Sie in das Eingabefeld eintragen und ebenfalls zur Adressliste hinzufügen. Dabei sind die Wildcards * (Stern) und ? (Fragezeichen) möglich. Trennen Sie die einzelnen Einträge durch einen Absatz (Enter-Taste).

Sollten Sie eine umfangreiche Liste von eigenen Adressen angelegt haben, so können Sie nach dort enthaltenem Text suchen, indem Sie auf das Symbol klicken. Die Textsuche steht Ihnen auch in den **Wortlisten** zur Verfügung. Nähere Informationen zu Suchen und Ersetzen finden Sie unter “Textsuche in Wortlisten” auf Seite 274.

Um einen Eintrag wieder aus der Liste zu löschen, markieren Sie diesen und klicken Sie auf **Entfernen**.

6. Klicken Sie **OK**.

7. Ihre Adressliste müsste nun etwa so aussehen:



Adressen dürfen aus Quarantäne hinzugefügt werden: Legen Sie hier fest, ob für diese Adressliste der direkte Zugriff aus einer Quarantäne-Mail heraus freigegeben ist. Wenn Sie im iQ.Suite Monitor in einer Quarantäne eine Mail ansehen, so können Sie durch die Schaltfläche **Hinzufügen** die Absenderadresse der Quarantäne-Mail zu verschiedenen Adresslisten hinzufügen. Im Auslieferungsstandard sind folgende Adresslisten für den direkten Zugriff freigegeben:

- Anti-Spam: Blacklist
- Anti-Spam: Newsletter Blacklist
- Anti-Spam: Newsletter Whitelist
- Anti-Spam: Whitelist

8. Klicken Sie noch einmal **OK**.

Ihre Adressliste ist nun angelegt und kann unter dem Menüpunkt **Adresslisten** geändert und gelöscht werden. Zum Löschen markieren Sie die Adressliste mit der rechten Maustaste und wählen Sie **Löschen** aus dem Kontextmenü.

6.5.4.2 Einsatz und Handhabung in einem Job

In jedem Job können Sie unter der Registerkarte **Adressen** bestimmen, für welche Benutzer ein Job gültig ist. Damit lassen sich Unternehmens-Richtlinien[6] einfach verwirklichen:

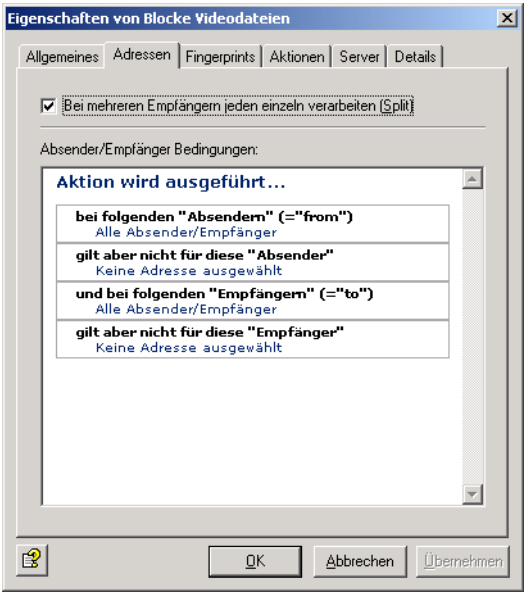
- **Bei folgenden Absendern** prüft den/die Absender. Die Ausnahme **Gilt aber nicht für diese Absender** ebenfalls.
- **und bei folgenden Empfängern** prüft den/die Empfänger. Die Ausnahme **Gilt aber nicht für diese Empfänger** ebenfalls.

Ein Beispiel für einen Job, der Dateianhänge blockt

Unternehmensrichtlinie: Es sollen keine Mails über das Internet ins Unternehmen gelangen, die Videoanhänge enthalten. Eine Ausnahme dieser Regel soll aber für das Marketing und die Geschäftsleitung definiert werden.

Umsetzung: Die Adresseinstellungen im Job müssen wie folgt aussehen: Die definierte Aktion im Job (also das Blocken der Anhänge) wird ausgeführt **bei folgenden Absendern**: <Externe Absender/Empfänger> und soll unter **und bei folgenden Empfängern** an <Interne Absender/Empfänger> gesendet werden. Unter **Gilt aber nicht für diese Empfänger** definieren Sie als Ausnahme die Abteilungen Marketing und Geschäftsleitung, die Sie entweder bereits im Active Directory als Gruppe eingetragen haben oder die Sie separat als eigene Adressliste anlegen können. Damit werden alle Videoanhänge abgefangen, die von externen Absendern an interne Empfänger gesendet werden, es sei denn, der Empfänger ist ein Mitarbeiter des Marketing oder ein Mitglied der Geschäftsleitung. Die Darstellung der Adresseinstellungen im Job:

6. siehe auch “Richtlinien-Konfiguration” auf Seite 118

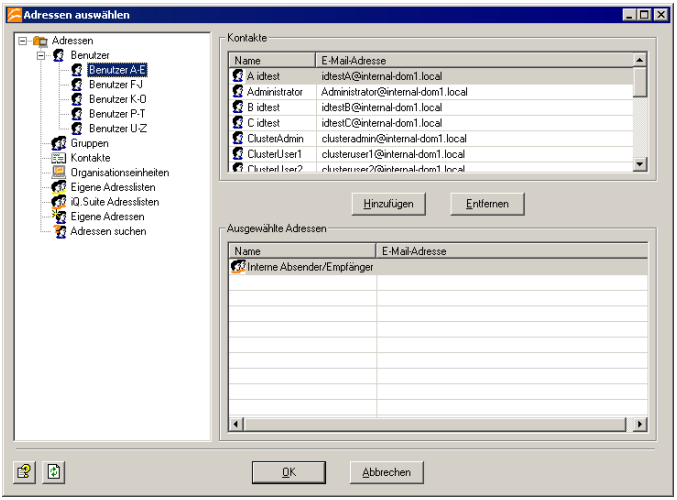


Bei mehreren Empfängern jeden einzeln verarbeiten (Split): Wenn eine E-Mail an mehrere Empfänger adressiert ist, und einer oder mehrere davon in einem Job in der Adressprüfung (**bei folgenden Empfängern/gilt aber nicht für ...**) eingetragen sind, wird diese eine E-Mail in zwei E-Mails aufgesplittet: eine E-Mail für die definierten Empfänger der Adressprüfung und eine für die nicht definierten Empfänger. Der Job behandelt dann nur die E-Mail mit den Empfängern, die definiert sind. Es wird **nicht** gesplittet, wenn Sie keine Adressprüfung für

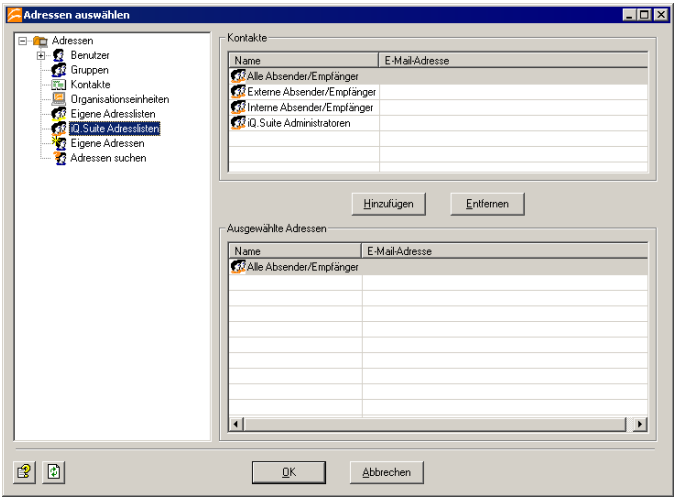
Empfänger definiert haben! Das Splitten der Mails hat Auswirkungen auf die Performance Ihres Servers.

Grundsätzlich müssen alle angegebenen Bedingungen in den Feldern **bei folgenden Absendern** und **bei folgenden Empfängern** zutreffen, damit eine Aktion ausgelöst wird (**und**-Verknüpfung!). Wenn mehrere Adressen innerhalb der gleichen Bedingung (z.B. **bei folgenden Absendern**) eingetragen sind, muss nur eine zutreffen, um die Aktion auszulösen. Die Ausnahmen (**gilt aber nicht für ...**) sind für die grundsätzliche Aktionsauslösung irrelevant. Mails für oder von diesen Ausnahmeadressen werden nur weitergereicht, ohne dass die definierten Aktionen ausgeführt werden.

Klicken Sie auf **Interne Absender/Empfänger**, **Keine Adresse ausgewählt** oder einen entsprechenden Eintrag in den Ausnahmen, um das Adressauswahlfenster aufzurufen und die Adressen für genau diese Bedingung zu definieren:



Die **iQ.Suite Adresslisten** stehen Ihnen ebenfalls zur Verfügung:



Die iQ.Suite Adresslisten sind feststehende Listen, aus den Einstellungen der übergreifenden **iQ.Suite Servers** generiert, die bei der Installation abgefragt und eingetragen werden oder die Sie manuell konfiguriert haben. Siehe dazu "Definition der E-Mail-Adressen und internen Domänen" auf Seite 21.

Eigene Adresslisten und **iQ.Suite Adresslisten** werden nur bei der Adressauswahl für einen Job angezeigt. Eigene Adresslisten können Sie jederzeit ändern, iQ.Suite Adresslisten können nicht geändert werden.

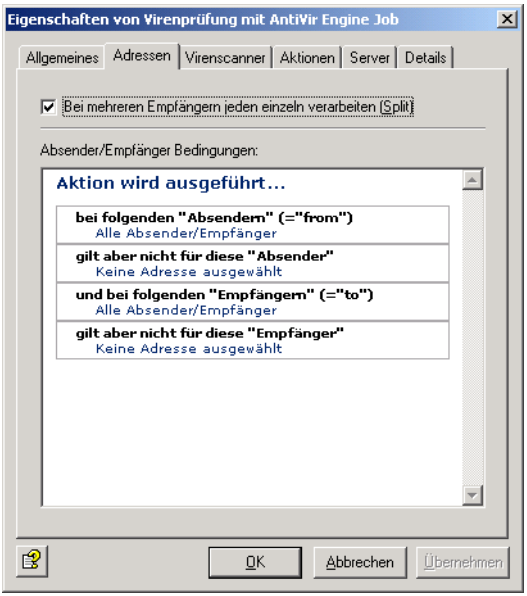
Nachfolgend noch einige kleinere Beispiele für Adresseinstellungen in einem Job.

Beispiel Viren prüfen

Unternehmensrichtlinie: Es sollen alle Mails auf Viren geprüft werden. In diesem Fall kann es nicht genügen, die Mails nur von externen Absendern zu prüfen. Es muss auch sichergestellt werden, dass keine infizierte Mail das Unternehmen verlässt. Die definierten Aktionen (Prüfen auf Viren, ggf. Reinigen der Datei und Kopieren in die Quarantäne) müssen also unabhängig von Absender oder Empfänger durchgeführt werden.

Umsetzung: Aktion wird ausgeführt **bei folgenden Absendern**: <Alle Absender/Empfänger> **und bei folgenden Empfängern** <Alle Absender/Empfänger>. Es gibt keinerlei Ausnahmen. Jede Mail von jedem Absender an jeden Empfänger wird auf Viren geprüft.

Die Darstellung der Adresseinstellungen im Job:

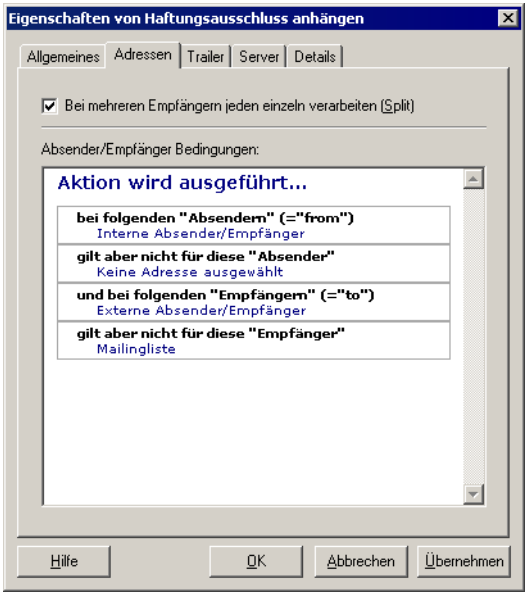


Beispiel Anfügen eines Haftungsausschluss

Unternehmensrichtlinie: An jede ausgehende E-Mail soll ein Haftungsausschluss oder eine Firmenankündigung angefügt werden, es sei denn, die Mail geht an eine Mailingliste. Interne E-Mails werden dabei ausgenommen.

Umsetzung: Die Aktion wird ausgeführt[7] **bei folgenden Absendern** <Alle internen Absender/Empfänger> **und bei folgenden Empfängern** <Alle externen Absender/Empfänger>. Unter den Ausnahmen **Gilt nicht für diese Empfänger** tragen Sie die in Ihrem Unternehmen aktiven Mailinglisten ein, indem Sie dafür eine eigene Adressliste erstellen und diese als Ausnahme angeben.

Die Darstellung der Adresseinstellungen im Job:



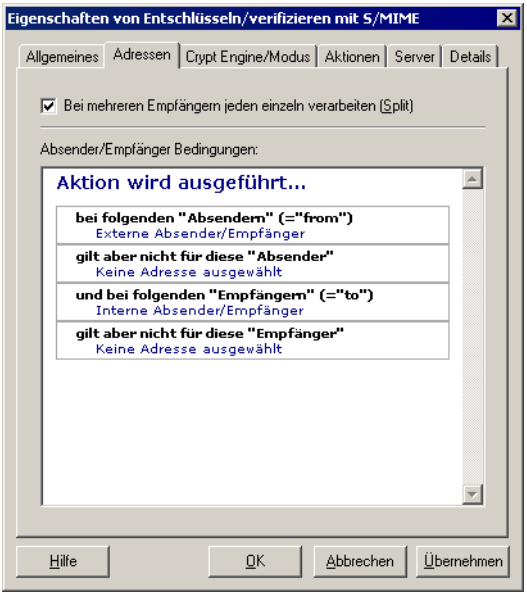
7. BeimTrailer -Job gibt es keine Registerkarte **Aktionen**, sondern der Jobzweck, also das Anhängen eines Trailers ist die Aktion.

Beispiel Entschlüsselung

Unternehmensrichtlinie: Eine Entschlüsselung findet grundsätzlich nur für eingehende E-Mails statt (eine Verschlüsselung nur für ausgehende E-Mails). Sinnvoll ist diese Einstellung aber nur, wenn Ihr Unternehmen mit allen Kontakten verschlüsselt kommuniziert oder grundsätzlich mit optionaler Verschlüsselung arbeitet[8].

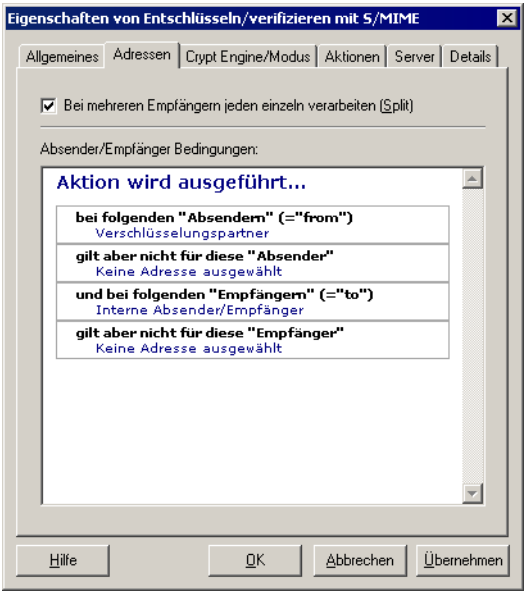
Umsetzung: Die Aktion bei Entschlüsselung wird also ausgeführt[9] **bei folgenden Absendern** <Alle externen Absender/Empfänger> **und bei folgenden Empfängern** <Alle internen Absender/Empfänger>.

Die Darstellung der Adresseinstellungen im Job:



8. siehe dazu "E-Mails mit PGP/GnuPG verschlüsseln - Jobbeispiel" auf Seite 151
9. Auch bei der Verschlüsselung und Entschlüsselung gilt als Aktion zunächst einmal der Jobzweck, also das Verschlüsseln bzw. Entschlüsseln. Die Registerkarte Aktionen definiert nur die Handhabung bei einem evtl. auftretenden Fehler.

Wenn Sie mit sicheren VPN-Kanälen[10] kommunizieren, ist der Einsatz von eigenen Adresslisten sinnvoller. Beispielsweise so:



Zusätzliche Informationen über Adressen, deren Eingabemöglichkeiten und über die Adressprüfung in iQ.Suite Wall finden Sie auch im Kapitel "Adressprüfung" auf Seite 266.

6.5.5 Benachrichtigungsvorlagen erstellen

In jedem Job können Sie unter **Aktionen** bestimmen, wer eine Benachrichtigung erhalten soll, wenn die iQ.Suite eine verbotene E-Mail entdeckt hat. Beim Anlegen eines neuen Jobs könenn Sie die entsprechende Vorlage für den Jobtyp auswählen. Nähere Informationen zu den einzelnen Jobtypen erhalten Sie unter "Richtlinien-Konfiguration" auf Seite 118.

Die Benachrichtigungsvorlagen für die einzelnen Jobs (Inhaltsprüfung, Virenprüfung usw.) erstellen Sie in der **Basis-Konfiguration**.

10. siehe dazu "Crypt Modus auswählen - Verschlüsselungsmodus - VPN" auf Seite 155

Vorkonfigurierte Benachrichtigungsvorlagen für die einzelnen Module finden Sie unter **Basis-Konfiguration --> Allgemeine Einstellungen --> Vorlagen**.

1. Klicken Sie auf **Vorlagen** und wählen Sie den Vorlagentyp.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf die gewünschte Vorlage und wählen Sie **Eigenschaften**.
3. Geben Sie den **Betreff** ein.
4. Klicken Sie auf die Registerkarte **Benachrichtigungstext --> Bearbeiten** für den Text der Benachrichtigung. Zur Gestaltung des Textes können Sie die Menüleiste für formatierten Text verwenden, die intern in HTML-Befehle umgewandelt werden. Wenn Sie den Quelltext mit der Schaltfläche aufrufen, können Sie die HTML-Befehle auch direkt eingeben.
5. Aus der Registerkarte **Jobs** ersehen Sie, in welchen Jobs die Benachrichtigungsvorlage verwendet wird.
6. Klicken Sie **OK**.

Näheres zum Vorlagentyp **Quarantäne-Sammelbenachrichtigungen** finden Sie in "Quarantäne-Sammelbenachrichtigungen einrichten" auf Seite 111.

6.5.5.1 Liste der Benachrichtigungsvariablen

Folgende Variablen, die Sie auch direkt mit dem Pfeil neben der Schaltfläche einfügen können, sind in den Benachrichtigungstexten und in den Betreffzeilen der Benachrichtigungen möglich:

Allgemeine	
[VAR]From[/VAR]	**Allgemein: Absender** Absender der aktionsauslösenden Mail
[VAR]Subject[/VAR]	**Allgemein: Betreff** Betreffzeile der aktionsauslösenden Mail
[VAR]Date[/VAR]	**Allgemein: Datum und Uhrzeit** Datum und die Uhrzeit, an dem der aktionsauslösende Job lief
[VAR]DateOnly[/VAR]	**Allgemein: Datum** Datum, an dem der aktionsauslösende Job lief

Allgemeine	
[VAR]Recipients[/VAR]	**Allgemein: Empfänger** Empfänger der aktionsauslösenden Mail
[VAR]Jobname[/VAR]	**Allgemein: Job Name** Name des Jobs, der eine Aktion auslöste
[VAR]Quarantine[/VAR]	**Allgemein: Quarantäneordner** Die Quarantäne, in die eine Mail gestellt wurde
[VAR]Server[/VAR]	**Allgemein: Server** Server, über den die betroffene Mail gesendet wurde, hier der Name, der in der Konfiguration eingetragen wurde.
[VAR]ServerFQDN[/VAR]	**Allgemein: Server (Netzwerkname)** Server, über den die betroffene Mail gesendet wurde, hier der Netzwerkname des Servers (Fully qualified domain name).
[VAR]TimeOnly[/VAR]	**Allgemein: Uhrzeit** Uhrzeit, zu der der aktionsauslösende Job lief
[VAR]ToolReport[/VAR]	**Allgemein: iQ.Suite Report** Kurze Zusammenfassung der Prüfungsergebnisse
[VAR]ToolReportDetails[/VAR]	**Allgemein: iQ.Suite Report (Details)** Ergebnis der Prüfungen mit allen Details

Für iQ.Suite Watchdog	
[VAR]AttachmentSize[/VAR]	**Watchdog: Anhanggröße** Größe des verbotenen/betroffenen Anhangs
[VAR]FingerprintName[/VAR]	**Watchdog: Anhangtyp** Name des verbotenen Dateityps
[VAR]Fingerprintcategory[/VAR]	**Watchdog: Fingerprintkategorie** Kategorie des verbotenen Dateityps
[VAR]MessageSize[/VAR]	**Watchdog: Gefundene E-Mail-Größe** Größe der gesamten E-Mail
[VAR]AttachmentName[/VAR]	**Watchdog: Gefundener Anhang** Namen der verbotenen/betroffenen Anhänge
[VAR]SetSizeLimit[/VAR]	**Watchdog: Max. E-Mail-Größe** Im Job festgelegte maximale Mailgröße
[VAR]Virusname[/VAR]	**Watchdog: Virusname** Namen der gefundenen Viren
[VAR]VirusScanner[/VAR]	**Watchdog: Virenscanner** Namen der fündig gewordenen Viren-scanner
Informationsspeicher-Scan	
[VAR]VSAPI_Database[/VAR]	**IS-Scan: Datenbank** Name des Informationsspeichers, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat

Für iQ.Suite Watchdog	
[VAR]VSAPI_Url[/VAR]	**IS-Scan: Datenbank URL** URL des Informationsspeichers, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
[VAR]VSAPI_ErrorText[/VAR]	**IS-Scan: Fehlerbeschreibung** Nähere Beschreibung im Fehlerfall durch den Informationsspeicher-Job
[VAR]VSAPI_SubmitTime [/VAR]	**IS-Scan: Gesendet am** Sende-Datum und -Uhrzeit der Nachricht
[VAR]VSAPI_MessageUrl [/VAR]	**IS-Scan: Nachrichten URL** Informationsspeicher-URL der Nachricht zum Zeitpunkt der Virenprüfung
[VAR]VSAPI_Folder[/VAR]	**IS-Scan: Ordner** Name des Informationsspeicher-Ordners, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
[VAR]VSAPI_Mailbox[/VAR]	**IS-Scan: Postfach** Name des Besitzers des Postfaches, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
[VAR]VSAPI_Server[/VAR]	**IS-Scan: Server** Name der Servers, auf dem die Virenprüfung durch den Informationsspeicher-Scan durchgeführt wurde
[VAR]virusscanner[/VAR]	**IS-Scan: Virenscanner** Namen des fündig gewordenen Virenscanners

Für iQ.Suite Watchdog	
[VAR]virusname[/VAR]	**IS-Scan: Virusname** Name der gefundenen Viren
[VAR]VSAPI_DeliveryTime [/VAR]	**IS-Scan: Zugestellt am** Zustell-Datum und -Uhrzeit der Nachricht

Für iQ.Suite Wall	
Inhaltsprüfung	
[VAR]DeniedContentTabHTML [/VAR]	**Wall: Details Inhaltsprüfung** Detailinformationen über die gefundenen Wörter/Phrasen
[VAR]DeniedMailParts[/VAR]	**Wall: Mailabschnitt** Betroffene aktionsauslösende Anhänge/ Nachrichtentexte
[VAR]DeniedWordlists[/VAR]	**Wall: Verbotene Wortlisten** Aktionsauslösende Wortlisten mit erreichtem Wert / Schwellwert
[VAR]DeniedWord[/VAR]	**Wall: Verbotener Inhalt** Aktionsauslösendes Wort mit erreichtem Wert / Schwellwert
Anti-Spam-Prüfung	
[VAR]CORECategory[/VAR]	**Wall: CORE Klassifizierungskategorie** Kategorie, in die die Mail durch CORE einsortiert (klassifiziert) wurde. Beispiel: HAM, SPAM

Für iQ.Suite Wall	
[VAR]COREPrediction[/VAR]	**Wall: CORE Klassifizierungsergebnis** Genauer Wert, inwieweit die Mail zu einer Klassifizierungskategorie gehört
[VAR]DCCString[/VAR]	**Wall: DCC Ergebnis** Rückgabewert des DCC-Servers, nachdem die Mail durch den Server analysiert wurde
[VAR]SpamReportHTML[/VAR]	**Wall: Details Spam-Analyse** Detailinformationen der einzelnen Spam-Kriterien
[VAR]SpamValue[/VAR]	**Wall: Spam-Wahrscheinlichkeit** Ermittelte Spam-Wahrscheinlichkeit in Form eines Wertes (0 - 100). Dieser Wert wird mit den individuell einzustellenden Schwellwerten im Advanced Spam Filtering Job verglichen.
[VAR]SpamLevel[/VAR]	**Wall: Spam-Level** Im E-Mail-Header jeder geprüften Mail wird von iQ.Suite Wall ein Spam-Level in Form von Sternen in 10er-Schritten eingetragen (z.B.: (X-SPAM-TAG: * bedeutet, Spam-Wahrscheinlichkeit liegt zwischen 0 und 10, X-SPAM-TAG: *** zwischen 20 und 30). Sie können nach diesem String im Header von Outlook suchen lassen und eine Regel formulieren, die z.B. alle Mails mit 3 und mehr Sternen mit diversen Aktionen belegt. Nähere Informationen über Regelmöglichkeiten in Outlook entnehmen Sie bitte der Outlook-Hilfe.

Für iQ.Suite Wall	
Adressprüfung	
[VAR]NumberRecipient[/VAR]	**Wall: Anzahl der Empfänger** Anzahl der adressierten Empfänger
[VAR]SetRecipientLimit[/VAR]	**Wall: Max. Empfängeranzahl** Im Job festgelegte Empfänger-Anzahl-Beschränkung
[VAR]DeniedSender[/VAR]	**Wall: Verbotene Absender** Name der aktionsauslösenden Absender
[VAR]DeniedRecipient[/VAR]	**Wall: Verbotene Empfänger** Name der aktionsauslösenden Empfänger
Sammelbenachrichtigung	
[VAR]From[/VAR]	**Sammelbenachrichtigung: Absender** Absender der Sammelbenachrichtigung.
[VAR]ReplyTo[/VAR]	**Sammelbenachrichtigung: Antwortadresse** Die Adresse, an die Antworten auf die Sammelbenachrichtigung geschickt werden sollen (NotificationReplyTo).
[VAR]Subject[/VAR]	**Sammelbenachrichtigung: Betreff** Betreff der Sammelbenachrichtigung.
[VAR]Nowdate[/VAR]	**Sammelbenachrichtigung: Datum aktuelle Sammelbenachrichtigung** Datum der Generierung der aktuellen Sammelbenachrichtigung.
[VAR]Lastdate[/VAR]	**Sammelbenachrichtigung: Datum letzte Sammelbenachrichtigung** Datum der Generierung der letzten Sammelbenachrichtigung

Für iQ.Suite Wall	
[VAR]Now[/VAR]	**Sammelbenachrichtigung: Datum und Zeit aktuelle Sammelbenachrichtigung** Datum und Uhrzeit der Generierung der aktuellen Sammelbenachrichtigung.
[VAR]Last[/VAR]	**Sammelbenachrichtigung: Datum und Zeit letzte Sammelbenachrichtigung** Datum und Uhrzeit der Generierung der letzten Sammelbenachrichtigung.
[VAR]RcptTo[/VAR]	**Sammelbenachrichtigung: Empfänger** Empfänger der Sammelbenachrichtigung.
[VAR]FQDN[/VAR]	**Sammelbenachrichtigung: Fully Qualified Domain Name** Voller Netzwerkname des Servers, auf dem sich die Quarantäne befindet, für die die Sammelbenachrichtigungen erzeugt werden.
[VAR]HtmlList[/VAR]	**Sammelbenachrichtigung: Liste der Quarantäne-Mails** Komplette Liste aller Quarantäne-Objekte für den entsprechenden Empfänger mit HTML-Formatierungen (Pflichtfeld in der Quarantäne-Sammelbenachrichtigung).
[VAR]HTTPPort[/VAR]	**Sammelbenachrichtigung: HTTP-Port** Port des HTTP-Servers.
[VAR]HTTPServer[/VAR]	**Sammelbenachrichtigung: HTTP-Server** HTTP-Server, um eine Benutzeranfrage per HTTP zu versenden.
[VAR]Displayname[/VAR]	**Sammelbenachrichtigung: Quarantäne** Name der Quarantäne, aus der die Liste der Mails erstellt wurde.

Für iQ.Suite Wall	
[VAR]Server[/VAR]	**Sammelbenachrichtigung: Server** Kurzname des Servers, auf dem sich die Quarantäne befindet, für die die Sammelbenachrichtigungen erzeugt werden
[VAR]Nowtime[/VAR]	**Sammelbenachrichtigung: Uhrzeit aktuelle Sammelbenachrichtigung** Uhrzeit der Generierung der aktuellen Sammelbenachrichtigung.
[VAR]Lasttime[/VAR]	**Sammelbenachrichtigung: Uhrzeit letzte Sammelbenachrichtigung** Uhrzeit der Generierung der letzten Sammelbenachrichtigung

Für iQ.Suite Crypt	
[VAR]Crypt_Security[/VAR]	**Crypt: Analyse-Ergebnisse** Anzeige des durchgeführten Crypt-Modus und dessen Ergebnisses (Mail war ver- bzw. nicht verschlüsselt ...)
[VAR]Crypt_NumberImported[/VAR]	**Crypt: Anzahl importierter Schlüssel** Anzahl der importieren Schlüssel. (Gezählt werden die Mail-Abschnitte, aus denen die Schlüssel importiert wurden.)
[VAR]Crypt_Engine[/VAR]	**Crypt: Crypt Engine** Name der konfigurierten Crypt Engine

Für iQ.Suite Crypt	
[VAR]Crypt_Method[/VAR]	**Crypt: Crypt Methode** Name der Verschlüsselungsmethode (PGP, S/MIME oder PGP/MIME)
[VAR]Crypt_Handling[/VAR]	**Crypt: Crypt Modus** Eingestellte Sicherheit im Job: Verschlüsseln, Signieren, Verschlüsseln und Signieren ...

Bitte beachten Sie, dass die Tokens *[VAR]* und *[/VAR]* case-sensitiv sind und immer in Großbuchstaben geschrieben werden müssen.

Nähere Informationen zu den Möglichkeiten und zur Syntax der Variablen finden Sie in “Erstellen eines neuen Trailers für individuelle Signaturen” auf Seite 203.

6.5.6 Trailer

iQ.Suite Trailer verwendet Trailer-Dokumente, um automatisch Text an ausgehende E-Mails anzuhängen. Diese Trailer werden in der Basis-Konfiguration erstellt und gepflegt. Nähere Informationen über das Hinzufügen und Ändern von Trailern finden Sie in “Erstellen eines neuen Textbaustein-Trailers” auf Seite 194 und “Erstellen eines neuen Trailers für individuelle Signaturen” auf Seite 203.

6.5.7 Ordner-Einstellungen

6.5.7.1 Quarantäne konfigurieren

Eine Quarantäne ist ein Ordner, in die alle von den Bedingungen betroffenen E-Mails abgelegt werden, wenn Sie das durch die Aktion **Kopie in Quarantäne** definiert haben. Bei der Installation der iQ.Suite wird im Datenverzeichnis ein Ordner namens **Quarantine** angelegt, in dem sich zunächst einige Standard-Quarantänen und später alle weiteren neu angelegten Quarantänen befinden. Unter dem Menüpunkt **Basis-Konfiguration --> Ordner-Einstellungen --> Quarantäne** können Sie die vorhandenen Quarantänen konfigurieren und neue einrichten.

1. Klicken Sie auf **Quarantänen**, im rechten Fenster werden alle verfügbaren Quarantänen angezeigt.
2. Klicken Sie mit der rechten Maustaste auf eine vorhandene Quarantäne im rechten Fenster und wählen Sie **Eigenschaften**.
3. Geben Sie eine Beschreibung für die Quarantäne ein.
4. Bestimmen Sie unter **Ordnername** den Ordnernamen der Quarantäne. Bitte hier keinen absoluten Pfad eingeben, sondern nur den Ordnernamen! Achtung: Diese Option erhalten Sie nur bei eigenen neu angelegten Quarantänen.

Eine neue Quarantäne legen Sie an, indem Sie mit der rechten Maustaste auf **Quarantäne** klicken und **Neu --> Quarantäne** wählen. Nach dem Speichern der Konfiguration werden diese Quarantänen automatisch vom EMH angelegt und werden anschließend auch im iQ.Suite Monitor angezeigt (aktualisieren Sie die Ansicht!).[11].

Die Größe einer Quarantäne ist auf 2 GB beschränkt! Achten Sie auf das Löschintervall. Automatisch gelöscht werden alle Einträge, die älter als 30 Tage sind (Standardeinstellung).

6.5.7.1.1 Quarantäne-Sammelbenachrichtigungen einrichten

Eine Quarantäne-Sammelbenachrichtigung informiert über die E-Mails, die von der iQ.Suite in die Quarantäne gestellt worden sind. Sammelbenachrichtigungen können an verschiedenste Empfänger(-gruppen) gesendet werden und eine Liste verschiedenster Quarantäne-Mails enthalten. Welche Mails das sind, welche Aktion der Empfänger der Sammelbenachrichtigung für diese Mails starten kann und welche Zusatzinformationen die Sammelbenachrichtigung enthält, wird in jeder Sammelbenachrichtigung separat konfiguriert.

Sammelbenachrichtigungen bestehen aus zwei Teilen: Aus der Vorlage (die Schablone oder der Rahmen), in der die Form der Sammelbenachrichtigung u.a. mit Variablen definiert wird und aus der Liste der quarantänierten Mails (der eigentliche Inhalt der Sammelbenachrichtigung), in der mit Feldern definiert wird, welche Mails und welche Felder der Mail in der erstellten Sammelbenachrichtigung aufgeführt werden sollen. Die Vorlage der Sammelbenachrichtigung wird

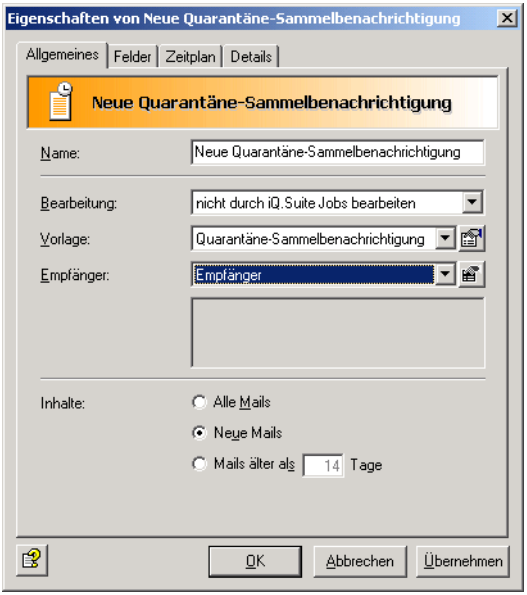
11. Weiteres über Quarantänen in “Quarantänen” auf Seite 124

unter **Basis-Einstellungen --> Vorlagen --> Quarantäne-Sammelbenachrichtigungen** mit Variablen eingestellt, welche ausschließlich die Sammelbenachrichtigung und ihre Form betreffen. Konfigurieren Sie die Quarantäne-Sammelbenachrichtigungsvorlage wie unter "Benachrichtigungsvorlagen erstellen" auf Seite 100 beschrieben. Der Inhalt der Sammelbenachrichtigung, also die Liste der Quarantäne-Mails, wird durch die Variable **Sammelbenachrichtigung: Liste der Quarantäne-Mails** ([VAR]HTMLList[/VAR]) definiert, die in jeder Sammelbenachrichtigung ein Pflichteintrag ist. Welche Einträge diese Liste enthält, wird unter **Ordner-Einstellungen --> Quarantänen --> Eigenschaften einer Quarantäne --> Felder** definiert. Konfigurierbar ist der Inhalt der Liste, nicht die Form bzw. Darstellung der Liste der Quarantäne-Mails.

Beispiel: Die Variable **Sammelbenachrichtigung: Absender** unter **Vorlagen** bezeichnet den Absender der Sammelbenachrichtigung (der gleiche Absender wie für alle Benachrichtigungen der iQ.Suite, wird unter **iQ.Suite Server-Einstellungen** definiert), die Checkbox für den **Absender** in der Registerkarte **Felder** in einer Quarantäne bezeichnet den Absender der quarantänierten E-Mail, welcher innerhalb der Liste der Mails aufgeführt wird.

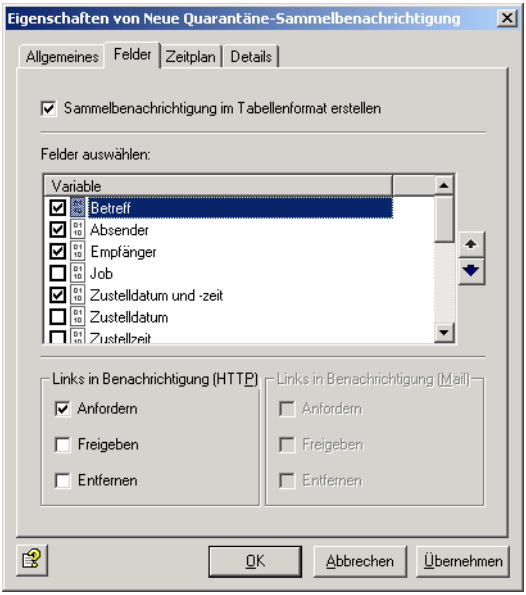
Sammelbenachrichtigungen sind insbesondere für Spam-Quarantänen und die Empfänger dieser Spam-Mails gedacht. Der Standardfall wird sein, dass die Anwender eine Liste aller neuen Spam-Mails erhalten, die an sie adressiert waren und die in einer bestimmten Spam-Quarantäne liegen. Die Konfiguration für diesen Standardfall:

1. Öffnen Sie **Basis-Konfiguration --> Ordner-Einstellungen --> Quarantäne**.
2. Öffnen Sie im rechten Fenster die Spam-Quarantäne **Anti-Spam: Mittel** mit Doppelklick.
3. Klicken Sie auf die Registerkarte **Sammelbenachrichtigungen**.
4. Klicken Sie auf **Hinzufügen**.
5. Vergeben Sie auf der Registerkarte **Allgemeines** einen **Name**n für die Sammelbenachrichtigung.



6. Wählen Sie im Feld **Empfänger** den Eintrag **Empfänger** aus. Empfänger der Sammelbenachrichtigung sind die ursprünglichen Empfänger der Quarantäne-Mails.
7. Als **Vorlage** können Sie eine Sammelbenachrichtigung wählen, die Sie unter **Allgemeine Einstellungen --> Vorlagen --> Quarantäne-Sammelbenachrichtigungen** selbst definiert haben. Im Auslieferungszustand der iQ.Suite ist nur die Vorlage **Quarantäne-Sammelbenachrichtigung** vorhanden.
8. Für die **Inhalte** der Sammelbenachrichtigung wählen Sie **Neue Mails**. Dadurch erhält der Empfänger der Sammelbenachrichtigung nur diejenigen Mails, die seit der letzten Sammelbenachrichtigung in der Quarantäne eingetroffen sind.
9. **Bearbeitung: nicht durch iQ.Suite Jobs bearbeiten** bedeutet, dass die erneut gesendete E-Mail, die der Benutzer angefordert oder freigegeben hat, nicht mehr durch die aktiven iQ.Suite Jobs geprüft wird. Jede angeforderte oder freigegebene E-Mail wird ungeprüft an die Empfänger zugestellt. Siehe hierzu auch die nächste Registerkarte **Felder**.

10. In der Registerkarte **Felder** wählen Sie aus, welche Felder aus den Quarantäne-Mails in die Liste der Quarantäne-Mails der Sammelbenachrichtigung geschrieben werden sollen. Markieren Sie hier beispielsweise die Checkbox **Betreff**, so wird der Betreff der Quarantäne-Mail in der Mail-Liste der Sammelbenachrichtigung aufgeführt. Für den Standardfall sind die entsprechenden Checkboxen bereits markiert.



Durch einen Klick auf die Links in der Benachrichtigung kann der Empfänger der Sammelbenachrichtigung eine Aktion mit der aufgeführten Mail durchführen. Markieren Sie hier die Aktion, die der Anwender durchführen darf:

Anfordern: Die Mail wird aus der Quarantäne an den Empfänger der Sammelbenachrichtigung zugestellt.

Freigeben: Die Mail wird an alle ursprünglichen Empfänger der Mail zugestellt.

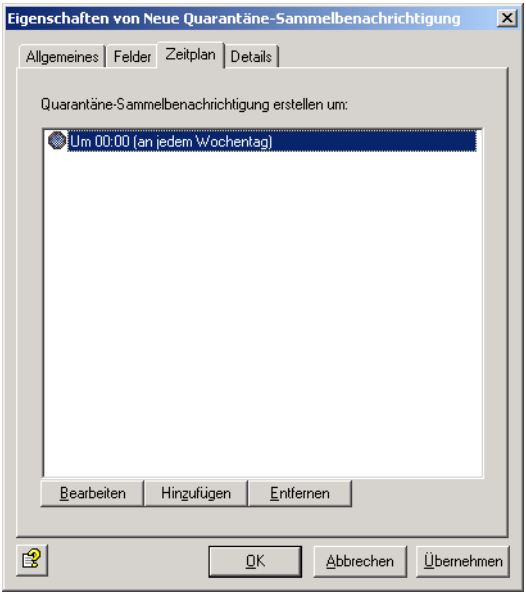
Entfernen: Die Mail wird in der Quarantäne zum Löschen vorgemerkt.

Wenn Sie mehrere Checkboxen aktiv setzen, so erscheinen in der Sammelbenachrichtigung mehrere Links an einer Mail.

11. Klicken Sie auf die Registerkarte **Zeitplan** und dort auf **Hinzufügen**. Sie erhalten ein Zeitplan-Fenster, in dem Sie den Start der Sammelbenachrichtigungserstellung definieren. In diesem Fall wird jeden Tag um 0 Uhr eine Sammelbenachrichtigung an die Empfänger der Spam-Mails erzeugt und gesendet.

Klicken Sie auf **OK**.

12. In der Registerkarte **Zeitplan** wird Ihre neue Quarantäne-Sammelbenachrichtigung jetzt angezeigt. Mit **Bearbeiten** ändern Sie die Zeit oder die Wochentage, mit **Entfernen** löschen Sie die Sammelbenachrichtigung:



Ab sofort wird täglich um 0 Uhr eine Sammelbenachrichtigung an die Empfänger von Spam-Mails der Quarantäne **Anti-Spam: Mittel** gesendet.

Sie können für eine Quarantäne mehrere verschiedene Sammelbenachrichtigungen mit unterschiedlichem Inhalt erstellen. Die Mails werden für jede Sammelbenachrichtigung separat aus der Quarantäne „zusamengesucht“, auch wenn der Zeitplan für diese Sammelbenachrichtigungen identisch ist.

6.5.7.2 Bridge

Näheres zu Bridge finden Sie unter “iQ.Suite Bridge” auf Seite 327.

6.5.8 Utility-Einstellungen

6.5.8.1 CORE Klassifikatoren

CORE Klassifikatoren werden von iQ.Suite Wall zur Spam-Erkennung und zur Inhaltsklassifikation verwendet. Für die Spam-Erkennung wird ein Klassifikator

mit der iQ.Suite ausgeliefert. Nähere Informationen über CORE finden Sie in “CORE Klassifikation” auf Seite 312.

6.5.8.2 Fingerprints

Fingerprints werden von iQ.Suite Watchdog zur Dateityperkennung benutzt. Wir liefern eine umfangreiche Liste von Fingerprints in der iQ.Suite mit aus, die in Kategorien eingeteilt sind. Im Regelfall ist es zunächst nicht nötig, Veränderungen vorzunehmen. Nähere Informationen über die Konfiguration von Fingerprints finden Sie in “Fingerprints konfigurieren” auf Seite 243.

6.5.8.3 Wortlisten

Hier können Sie Wortlisten erstellen, die diejenigen Textfolgen enthalten, die Sie bei der Inhalts- und Spamprüfung mit iQ.Suite Wall verbieten möchten. Wir liefern einige Wortlistenkategorien aus, die Sie an Ihre Bedürfnisse anpassen können. Die genaue Konfiguration der Wortlisten finden Sie in “Wortlisten einrichten” auf Seite 272.

6.5.8.4 Virenscanner

iQ.Suite Watchdog verwendet zur Virenprüfung **Virenscanner** von Drittherstellern. Alle Virenscanner mit Ausnahme des AntiVir von H+BEDV müssen vor der Installation der iQ.Suite auf Ihrem Server installiert sein. Näheres zur Installation finden Sie in “Installation der Virenscanner” auf Seite 25. Nähere Informationen zur Konfiguration der Virenscanner entnehmen Sie dem Kapitel “Virenscanner konfigurieren” auf Seite 216.

6.5.8.5 DCC

Die DCC-Technologie wird von iQ.Suite Wall zur Spam-Erkennung verwendet. Sie erkennt Massen-Mails mittels Prüfsummen, die von DCC-Servern gezählt werden. In der **Basis-Konfiguration** werden die übergreifenden DCC-Einstellungen vorgenommen. Nähere Informationen zu Anti-Spam mit DCC finden Sie unter “Anti-Spam mit Wall DCC Spam Filtering” auf Seite 307.

6.5.8.6 Crypt Engines

iQ.Suite Crypt verwendet zur Ver- und Entschlüsselung die Programme PGP, GnuPG oder S/MIME. Diese sogenannten **Crypt Engines** werden auf dem Server installiert und in der Basis-Konfiguration für die iQ.Suite konfiguriert. Näheres zur Konfiguration der einzelnen Engines finden Sie in “Konfiguration der PGP

bzw. GnuPG Crypt Engine" auf Seite 140 und in "Konfiguration der S/MIME Crypt Engine" auf Seite 168.

6.6 Richtlinien-Konfiguration

In der **Richtlinien-Konfiguration** definieren Sie Ihre iQ.Suite Jobs basierend auf firmeneigenen Richtlinien.

Anhand unterschiedlicher Bedingungen (oder auch Filter) können Sie festlegen, welche Mails überhaupt betroffen sind, wann welche Aktion ausgeführt werden soll und in welcher Reihenfolge die Jobs abgearbeitet werden sollen (Priorität). Alle Bedingungen können innerhalb der Jobs konfiguriert werden. Die Summe der iQ.Suite Jobs ergibt die Unternehmensrichtlinien (Policy).

6.6.1 Beispiel einer Unternehmensrichtlinie

Jede eingehende Spam-Mail soll erkannt, gelöscht und in die Quarantäne gestellt werden. Die Spam-Mails sollen den Empfänger zwar nicht erreichen, er soll aber darüber informiert werden, dass und welche Spams für ihn eingegangen sind, damit er selbst entscheiden kann, welche dieser Mails ihm doch zugestellt werden sollen. Dies sollte mittels einer Zusammenfassung geschehen, die einmal täglich versendet werden soll. Das alles können Sie in den **Wall Spam Filtering Jobs** einrichten.

6.6.2 Jobtypen

Es existieren 14 unterschiedliche Jobtypen, die Sie unter **Richtlinien-Konfiguration** --> **Mail Transport Jobs** --> rechte Maustaste **--> Neu** finden können:

Jobtyp	Bedeutung
Watchdog Virus Scanning	Job prüft die E-Mails auf Viren.
Watchdog Attachment Filtering	Job prüft die E-Mails auf verbotene Dateianhänge. Die verschiedenen Dateiformate werden durch Fingerprints identifiziert.
Watchdog Attachment/ Size Filtering	Job prüft die E-Mails auf verbotene Dateianhänge. Gleichzeitig kann die maximal zugelassene Größe eines Anhangs angegeben werden.

Jobtyp	Bedeutung
Watchdog E-Mail Size Filtering	Job prüft die E-Mails auf eine maximal zugelassene Größe (Angabe pro E-Mail).
Wall E-Mail Address Filtering	Job prüft die E-Mails auf Adresseinschränkungen.
Wall Content Filtering	Job prüft E-Mails und Anhänge auf verbotenen Textinhalt.
Wall Spam Filtering	Job prüft E-Mails mittels verschiedener Kriterien auf Spam.
Wall CORE Classification	Job klassifiziert die Mails nach Inhalten oder prüft die E-Mails mittels CORE auf Spam. Bei der Klassifizierung nach Inhalten ist die Erstellung eines neuen Klassifikators erforderlich. Verwenden Sie den Job bei Spamprüfungen nur für Testzwecke, die CORE-Prüfung ist im Wall Spam Filtering Job als kombiniertes Kriterium integriert und muss nur aktiviert werden.
Wall DCC Spam Filtering	Job prüft die E-Mails mittels eines DCC-Servers auf Spam. Dieser Job ist nur für Testzwecke gedacht, die DCC-Prüfung ist im Wall Spam Filtering Job als kombiniertes Kriterium integriert und muss nur aktiviert werden.
Wall Recipient Limit Filtering	Job prüft die E-Mails auf eine maximal zulässige Anzahl der Empfänger pro E-Mail (Gezählt werden die Empfänger im „to“-Feld einer Mail).
Trailer	Job hängt einen vorher erstellten und definierten Textbaustein an bestimmte oder alle ausgehenden E-Mails.
Crypt Key Import	Job importiert PGP Schlüssel automatisch in den öffentlichen Schlüsselbund.

Jobtyp	Bedeutung
Crypt Inbound	Job entschlüsselt oder verifiziert eingehende E-Mails mit PGP, GnuPG oder S/MIME.
Crypt Outbound	Job verschlüsselt oder signiert ausgehende E-Mails mit PGP, GnuPG oder S/MIME.

Für jeden Jobtyp können Sie eigene Bedingungen definieren, die **alle** zutreffen müssen, bevor eine definierte Aktion ausgeführt wird. Allen Jobtypen gemeinsam ist die Adressprüfung, die immer zusätzlich zur Verfügung steht. Sie können z.B. einen Job mit den Bedingungen erstellen, alle Mails, die von den Domänen *@gmx.net und *@hotmail.com gesendet werden, größer als 500 KB sind und der Fingerprintkategorie **Sound** angehören, zu löschen (und damit dem Empfänger nicht zuzustellen!) und eine Kopie davon in die Quarantäne zu stellen. Dieser Fall wäre ein **Watchdog Attachment/Size Filtering Job**.

Im Lieferumfang der iQ.Suite ist eine Reihe von Standardjobs enthalten, die Sie für Ihre Bedürfnisse ändern können. Selbstverständlich sind auch eigene möglich. Sie finden die vorkonfigurierten Jobs unter **Richtlinien-Konfiguration --> Jobbeispiele**. Ziehen Sie den gewünschten Job mit der Maus in **Mail Transport Jobs**. Es lassen sich beliebig viele Jobs anlegen. Die Reihenfolge der Abarbeitung ersehen Sie in **Mail Transport Jobs** aus der **Priorität** in der Liste aller Jobs. Neue Jobs werden in der Priorität immer hinten angehängt. Die Pfeiltasten und in der Symbolleiste ändern die Priorität jeweils um eine Stufe nach oben oder nach unten.[12]

Ein Job kann aktiv oder inaktiv sein. Ein inaktiver Job ist zwar in der Konfiguration vorhanden, kommt aber nicht zur Ausführung. Sie müssen also Ihre Jobs nicht endgültig aus der Konfiguration löschen, wenn Sie diese deaktivieren wollen.

In jedem Job können Sie unter der Registerkarte **Aktionen** einstellen, welche Aktionen zur Ausführung kommen sollen, wenn eine E-Mail unter die definierten Bedingungen fällt oder mit einem Virus verseucht ist.

12. siehe auch “Prioritäten der Jobs” auf Seite 122

6.6.3 Aktionen

Zusätzlich zu den Aktionen, die zur Funktion eines Jobs gehören, stehen Ihnen folgende Standard-**Aktionen** zur Verfügung:

Kopie in Quarantäne	Eine Kopie der E-Mail wird in den von Ihnen angegeben Quarantäne-Ordner gestellt, wo sie jederzeit eingesehen werden kann.
Lösche E-Mail	Die infizierte/verbotene Original-E-Mail wird endgültig vom Server gelöscht (die Kopie befindet sich in der Quarantäne, wenn die Option gesetzt ist).
Lösche Anhang	Die infizierten Anhänge werden endgültig vom Server gelöscht.
Zusatz im Betreff	Die Betreffzeile wird durch den Zusatz „Checked“ ergänzt. Damit ist diese E-Mail als bereits bearbeitet gekennzeichnet.
Sende Benachrichtigungen an	Benachrichtigungen können an folgende Personenkreise gesendet werden: ■ Administratoren ■ Absender ■ Empfänger ■ Andere Personen
Starte externe Anwendung	Eine externe, frei wählbare Anwendung wird ausgeführt.
X-Header Feld hinzufügen	Es wird im Header der E-Mail ein Feld hinzugefügt, welches mit einem Wert aus den Variablen gefüllt werden kann.
Mail umleiten	Die E-Mail wird an die angegebenen Empfänger umgeleitet. Option: Original-Empfänger erhalten die Mail zusätzlich.

6.6.4 Prioritäten der Jobs

Die Priorität eines Jobs wird in der Ansicht aller Jobs in der **Richtlinien-Konfiguration --> Mail Transport Jobs** angezeigt und bestimmt die Reihenfolge der Abarbeitung der Jobs. Für jede Priorität wird eine Kennziffer vergeben. Jeder neue Job erhält eine neue Kennziffer, die an die letzte Kennziffer anschließt. Die Jobs werden mit den Pfeiltasten und in der Symbolleiste oder mit rechter Maustaste (**Alle Tasks --> Nach oben/Nach unten)** in die gewünschte Reihenfolge gebracht. Die Kennziffern der Jobs ändern sich entsprechend. Wenn die Jobs nach der Spalte **Priorität** sortiert sind, werden sie in genau dieser Reihenfolge auch abgearbeitet.

Wird ein Job gelöscht, so rückt der nachfolgende Job in der Priorität und Kennziffer automatisch eins nach oben.

Sinnvolle Prioritätenvergabe:

Die höchste Priorität sollte ein Virenprüfungsjob erhalten. Mails, die vielleicht wieder aus der Quarantäne an den Empfänger zugestellt werden müssen (da diese Mail vom Empfänger evtl. doch gebraucht wird), dürfen keinen Virus enthalten. Die Mails, die wieder zugestellt werden könnten, sind z.B. die Mails aus Jobs mit Blockfunktionen für bestimmte Fingerprints oder aus Anti-Spam-Jobs, über die die Anwender per Sammelbenachrichtigung (siehe Seite 111) informiert werden und die sie sich zustellen lassen können. Wenn eine Mail z.B. durch einen Anti-Spam-Job in die Quarantäne gestellt wird, so wird die Aktion zwar durch den erkannten Spam ausgelöst und die Mail trägt in der Quarantäne das Label *Spam*, es kann aber nicht ausgeschlossen werden, dass diese Mail auch einen Virus enthält, wenn die Virenprüfung nicht vorher durchgeführt wurde.

Wir raten auch dazu, diejenigen Jobs, die einfache Blockfunktionen für z.B. sehr große Mails oder unbekannte Archive durchführen, mit hoher Priorität zu belegen, damit die betroffenen Mails keine weiteren Prüfungen durchlaufen müssen und somit den Server nicht mehr belasten können. Definieren Sie einen **Wall Recipient Limit** Job mit einer hohen Priorität, damit dieser Job schon einmal die Mails aussortiert, die an zu viele Empfänger adressiert sind, bevor ein Job läuft, der eine Adressprüfung macht und ggf. ein Splitting durchführt (siehe dazu auch

“Adresslisten” auf Seite 90). In einem solchen Fall kann der Recipient Limit Job nicht mehr korrekt ausgeführt werden, da die Anzahl der Empfänger bereits verändert worden ist.

6.7 iQ.Suite Monitor

Im iQ.Suite Monitor beobachten Sie alle **iQ.Suite Server**, **Quarantänen** und **Bad-Mails**. Außerdem haben Sie hier Zugriff auf die **Statistik Auswertungen**. Um auf einen Server zugreifen zu können, tragen Sie ihn zunächst unter **Basis-Konfiguration --> iQ.Suite Servers** ein und aktualisieren Sie den **iQ.Suite Monitor** in der Ansicht. Die Vorgehensweise entnehmen Sie bitte der Beschreibung “Einstellungen für einen einzelnen iQ.Suite Server” auf Seite 85. Außerdem sollte Ihre Quarantäne entsprechend der Beschreibung in Kapitel “Quarantäne konfigurieren” auf Seite 110 eingerichtet sein.

Der iQ.Suite Monitor erfordert außerdem eine Anmeldung als autorisierter Benutzer. Es erscheint ein Anmeldedialog, in dem Sie Ihren üblichen Benutzernamen und das Passwort für die entsprechende Domäne angeben.

Die Berechtigung für den iQ.Suite Monitor-Zugriff wird in den Eigenschaften der Datei **access.acl** im Ordner

```
..\GROUP Technologies\iQ.Suite\AppData\
```

eingetragen. Klicken Sie auf die Registerkarte **Sicherheit** und geben Sie den gewünschten Benutzern mindestens einen Lesezugriff. Bei der Installation der iQ.Suite wird die Berechtigungseinstellung des entsprechenden übergeordneten Laufwerks übernommen.

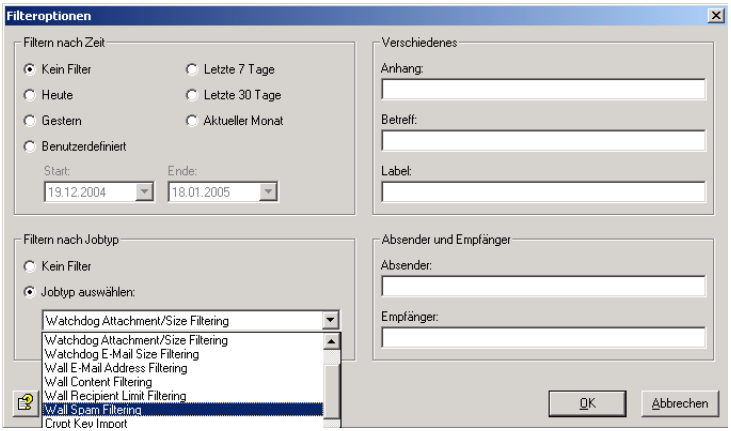
Der Anmeldedialog erscheint nur dann für einen anderen Server, wenn Ihr aktueller Benutzername auf dem zweiten Server keine ausreichende Berechtigung hat. Die Anmeldung auf mehreren Servern gleichzeitig mit verschiedenen Benutzernamen ist möglich. Das heißt, alle Logins sind gleichzeitig aktiv und sie können auf jeden iQ.Suite Monitor jeden Servers zugreifen.

Für jeden Server können Sie sich umfassende Informationen über die iQ.Suite Version, die Konfiguration u.a. anzeigen lassen. Klicken Sie im **iQ.Suite Monitor** mit der rechten Maustaste auf den gewünschten Server und wählen Sie **Eigenschaften**.

6.7.1 Quarantänen

Wenn Sie im Job die Aktion **Kopie in Quarantäne** aktiviert haben, befinden sich alle betroffenen E-Mails in einer Quarantäne[13] und Sie erhalten an dieser Stelle alle verfügbaren Informationen über die einzelnen Mails. Die Anzeige ist auf die neuesten 10.000 Mails beschränkt.

Innerhalb einer Quarantäne ist es möglich, die E-Mails nach etlichen Auswahlkriterien zu filtern. Klicken Sie dazu mit der rechten Maustaste auf **Ansicht --> Filteroptionen** oder auf das Icon . Sie erhalten folgenden Dialog:



Auch in dieser Filterliste werden bis zu 10.000 Mails angezeigt. Dadurch, dass Sie die Anzeige der Mails mit Filteroptionen einschränken, erhalten Sie also auch ältere Mails, die in der Liste aller Quarantäne-Mails nicht mehr aufgeführt werden.

Wollen sie die Optionen wieder zurücksetzen, haben Sie drei Möglichkeiten:

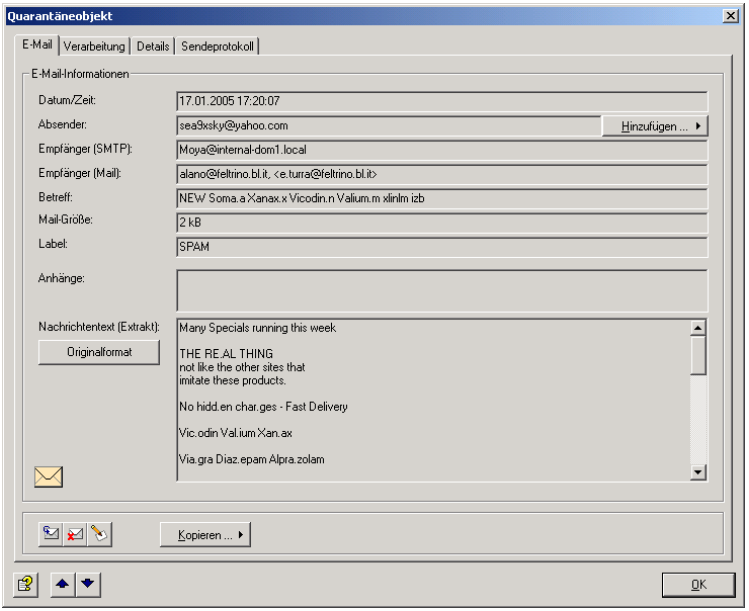
1. Aktivieren Sie die Option **Kein Filter** in **Filteroptionen**
2. Klicken Sie mit der rechten Maustaste auf **Ansicht**
   --> Alle Objekte anzeigen
3. Benutzen Sie das Icon in der Symbolleiste.

13. siehe dazu “Quarantäne konfigurieren” auf Seite 110

6.7.1.1 Beispiel einer E-Mail in der Quarantäne

Diese Informationen erhalten Sie, wenn Sie mit einem Doppelklick oder der rechten Maustaste die **Eigenschaften** der Mail in der Quarantäne aufrufen.

Unter der Registerkarte **E-Mail** finden Sie das Wichtigste auf einen Blick:



Die auf diesen Registerkarten verwendeten Icons:

E-Mail aus Quarantäne senden

E-Mail in Quarantäne löschen

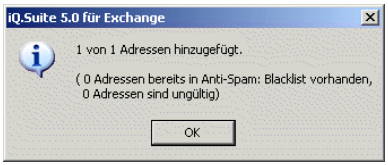
Label für die E-Mail festlegen, ändern, löschen

Nächste E-Mail in der Quarantäne/Badmail

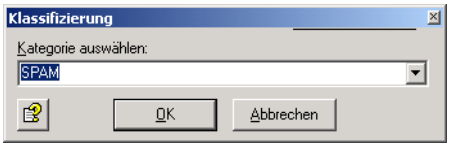
Vorherige E-Mail in der Quarantäne/Badmail

Die Schaltfläche **Hinzufügen** ermöglicht es, den Absender der Mail einer bestimmten Adressliste hinzuzufügen. Welche Adresslisten unter dieser Schaltfläche angezeigt werden, definieren Sie für jede einzelne Adressliste. Siehe

hierzu “Adresslisten” auf Seite 90. Sobald die Absenderadresse der Adressliste hinzugefügt worden ist, erhalten Sie eine Meldung:


iQ.Suite 5.0 für Exchange
1 von 1 Adressen hinzugefügt.
(0 Adressen bereits in Anti-Spam: Blacklist vorhanden,
0 Adressen sind ungültig)
OK

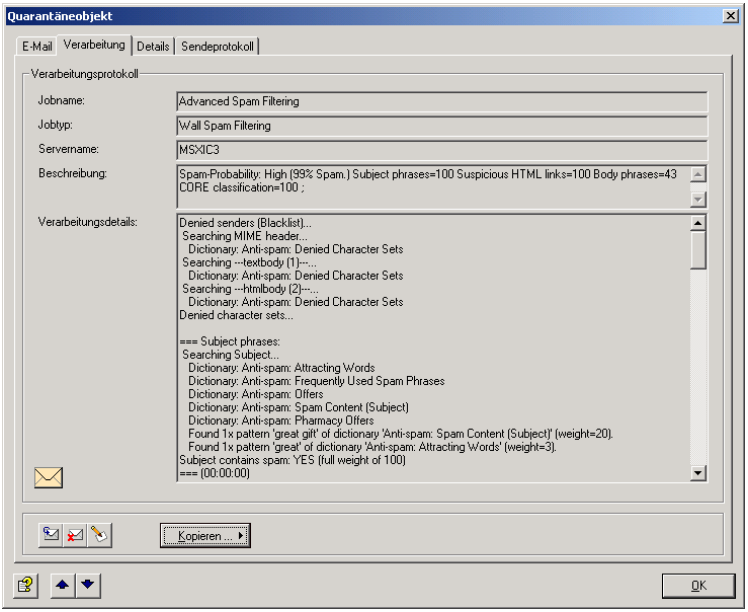
Die Schaltfläche **Kopieren** ermöglicht es, die Mail in eine andere auf diesem Server vorhandene Quarantäne zu kopieren. Sie können diese Mail hier auch einer CORE Klassifizierungskategorie[14] zuordnen. Der auf diesem Server vorhandene CORE Klassifikator wird als Auswahl zur Verfügung gestellt und Sie können eine Kategorie für diese Mail vergeben:



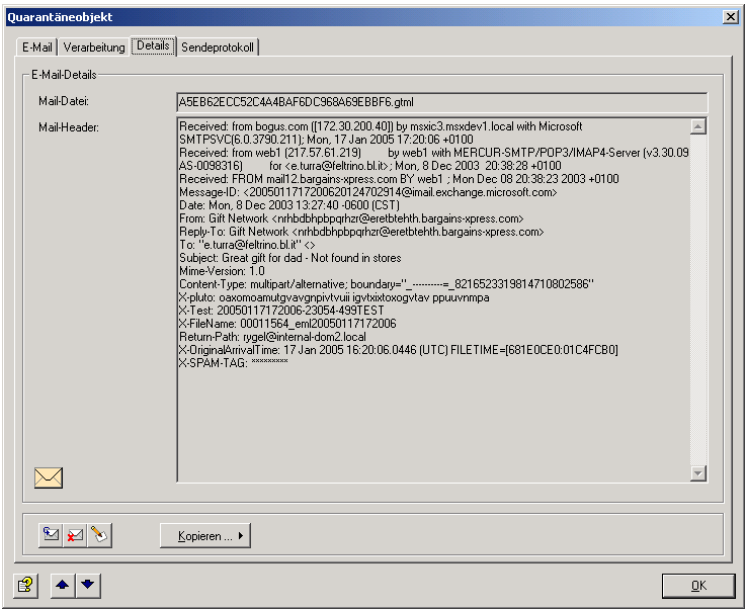
Anschließend finden Sie diese Mail in der entsprechenden Kategorie des CORE Klassifikators (**iQ.Suite Monitor --> Server -->** <Servername> **--> CORE Klassifikatoren -->** <Klassifikatorname> --> <Kategoriename>).

Unter **Verarbeitung** erfahren Sie den Namen des Jobs, der die E-Mail in die Quarantäne abgelegt hat, den Jobtyp, den Server, warum die Mail unter die Einschränkungen fiel und in die Quarantäne gestellt wurde und weitere Verarbeitungsdetails:

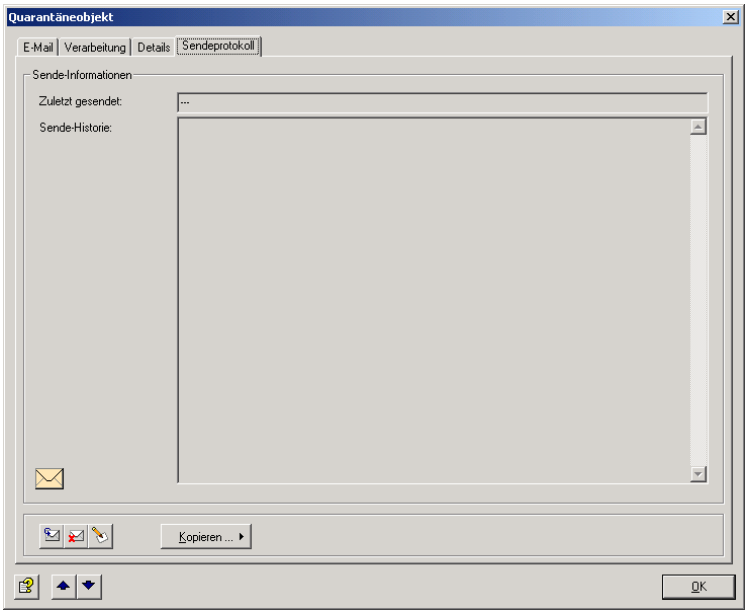
14. siehe “CORE Klassifikatoren” auf Seite 132



Unter **Details** wird der Dateiname der E-Mail und der Nachrichtenkopf angezeigt:



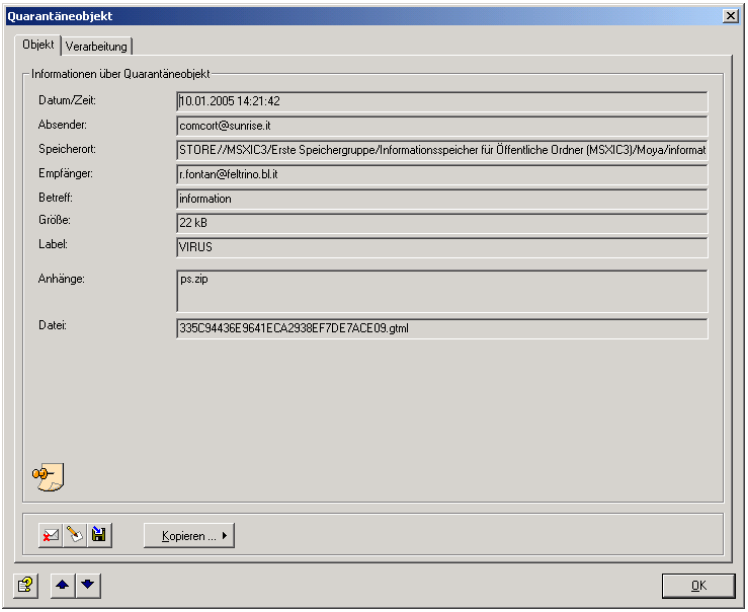
Unter **Sendeprotokoll** erhalten Sie den Verlauf des erneuten Sendens aus der Quarantäne.



6.7.1.2 Beispiel einer E-Mail in der Informationsspeicher-Quarantäne

Diese Informationen erhalten Sie, wenn Sie mit einem Doppelklick oder der rechten Maustaste die **Eigenschaften** der Mail in der Informationsspeicher-Quarantäne aufrufen.

Unter der Registerkarte **Objekt** finden Sie das Wichtigste auf einen Blick:



Die auf diesen Registerkarten verwendeten Icons:

Objekt in Quarantäne löschen

Label für das Objekt festlegen, ändern, löschen

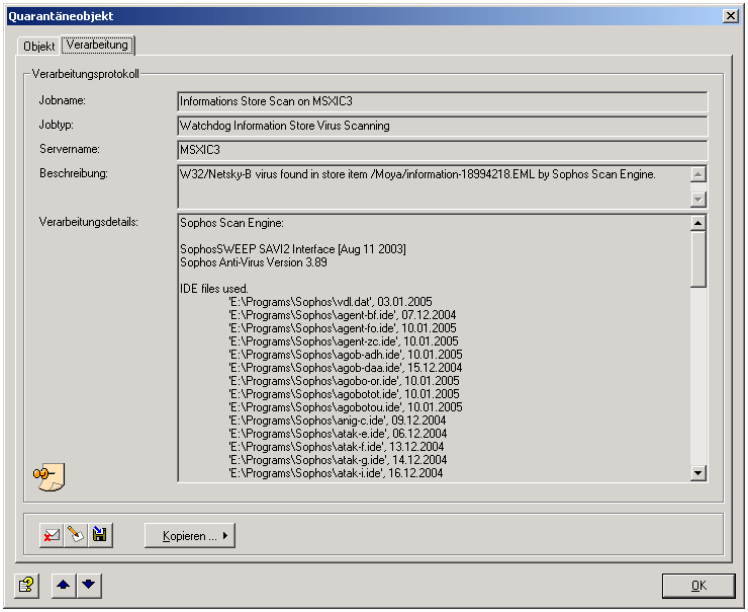
Objekt im Dateisystem speichern

Nächstes Objekt in der Quarantäne

Vorherige Objekt in der Quarantäne

Die Schaltfläche **Kopieren** ermöglicht es, das Objekt in eine andere auf diesem Server vorhandene Quarantäne zu kopieren.

Die nächste Registerkarte **Verarbeitung** zeigt den Namen des Jobs, der die E-Mail in die Quarantäne abgelegt hat, den Jobtyp, den Server, warum das Objekt unter die Einschränkungen fiel und in die Quarantäne gestellt wurde und weitere Verarbeitungsdetails:



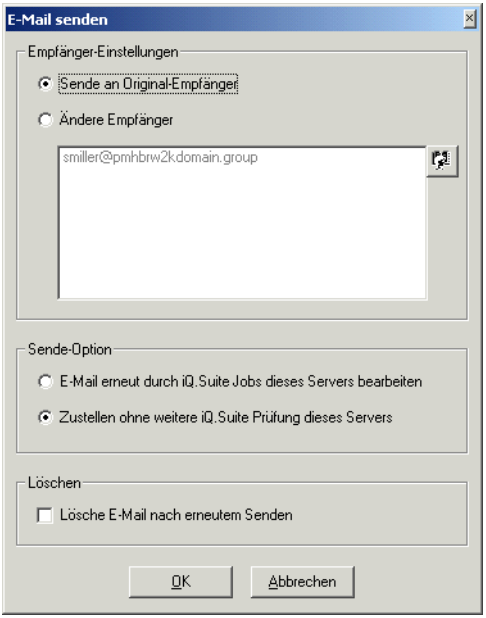
6.7.1.3 Aus Quarantäne senden

Wenn Sie eine E-Mail aus der Quarantäne wieder seinem ursprünglichen oder einem weiteren Empfänger zukommen lassen möchten, können Sie diese direkt aus der Quarantäne wieder versenden, ohne dass sie erneut von einem iQ.Suite Job geprüft wird:

1. Öffnen Sie eine Liste von Mails einer Quarantäne im iQ.Suite Monitor
2. Wählen Sie die gewünschte Mail mit der rechten Maustaste aus
3. Aktivieren Sie nun **Alle Tasks --> Aus Quarantäne senden**

Alternativ können Sie die Mail auch direkt aus dem Eigenschaften-Fenster versenden, indem Sie auf das Icon klicken.

4. Sie erhalten folgenden Dialog:



Der Empfänger sieht im „from“-Feld den Original-Absender der E-Mail (keine Weiterleitungsmail!). Sie können den Empfänger ändern, indem Sie die Option **Ändere Empfänger** aktivieren und dann auf das Symbol für Adresse auswählen klicken.

In der Auswahl der Adressen für das erneute Versenden aus der Quarantäne werden keine Adresslisten verwendet. Sie stehen daher nicht zur Verfügung. Näheres zu Adresslisten siehe “Adresslisten” auf Seite 90.

Wenn Sie die Mail nicht mehr durch die Jobs bearbeiten lassen möchten, so aktivieren Sie die Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers**. Das wird der Regelfall sein, denn wenn Sie eine Mail aus der Quarantäne wieder zustellen lassen, so ist das meist dann, wenn ein Benutzer diese Mail trotz z.B. verbotener Wörter oder Anhängen dringend braucht.

Es handelt sich hier um eine übergreifende Einstellung. Sollten Sie Jobs aktiviert haben, die auch erneut gesendete Mails aus der Quarantäne prüfen sollen, so setzen Sie diese Einstellung auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**, ansonsten greift die Jobeinstellung **Vor Versand prüfen** nicht und es werden **alle** Mails unbearbeitet weitergesendet.

Die Anweisung **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** gilt auch nur für diejenigen Jobs, bei denen die Option **Mails aus Quarantäne: Vor Versand prüfen** aktiviert worden ist! Selbst wenn Sie also die Quarantäne-Mails erneut bearbeiten lassen wollen, werden alle Jobs ausgeklammert, bei denen **Ohne Prüfung versenden** aktiviert ist.

6.7.1.4 Bad-Mails

Bad-Mails sind alle E-Mails, die durch die iQ.Suite Jobs nicht bearbeitet werden konnten, wie beispielsweise Mails mit nicht verarbeitbaren Formaten. Über Bad-Mails existieren sehr wenig Informationen, da die iQ.Suite keine Einsicht in diese Mails nehmen konnte. Diese Mails können also auch einen unentdeckten Virus enthalten.

Für Bad-Mails existiert auf jedem Server nur ein Ordner. Es können auch keine weiteren Ordner angelegt werden. Ansonsten gelten für Bad-Mails die gleichen Funktionen und Optionen wie für Quarantäne-Mails.

6.7.2 CORE Klassifikatoren

Die CORE Technologie wird zur Inhaltsprüfung und -klassifizierung mit iQ.Suite Wall verwendet. Dazu werden CORE Klassifikatoren eingesetzt, die die Mails in verschiedene Inhaltskategorien einteilen. An dieser Stelle können Sie Ihre CORE Klassifikatoren verwalten und anlernen. Unterhalb eines Klassifikators befinden sich die angelegten Kategorien mit den dazugehörigen Mails. Die Mails können Sie per Drag & Drop aus den Quarantänen in die einzelnen Kategorien des Klas-

sifikators kopieren und den Klassifikator anschließend anlernen, indem Sie mit der rechten Maustaste auf dem gewünschten Klassifikator **Alle Tasks --> Klassifikator anlernen** wählen. Näheres zur CORE Technologie und zur Verwendung von CORE Klassifikatoren finden Sie in "CORE Klassifikation" auf Seite 312.

6.7.3 iQ.Suite Reports

Mit Hilfe der Reporting- und Statistik-Funktion der iQ.Suite können detaillierte Informationen über die E-Mail-Verarbeitung abgerufen werden. Es stehen mehr als zehn Reports zur Verfügung. Die Reports sind über den iQ.Suite Monitor erreichbar. Die einzelnen Reports beinhalten sowohl die graphische Darstellung von erkannten Richtlinienverletzungen (z.B. Viren, unerwünschte Dateianhänge) als auch tabellarische Informationen. Zu jedem iQ.Suite Jobtyp steht ein eigener Report bereit. Darüber hinaus werden Daten zu iQ.Suite Quarantänen dargestellt. Die Reports können für frei definierbare Zeiträume erstellt werden. Umfangreiche Druck- und Exportfunktionalitäten ermöglichen die einfache Weiterverwendung der Reporting-Daten.

Die Report-Daten werden während der Verarbeitung zwischengespeichert und zwei Mal pro Stunde in die Auswertungsdatenbank geschrieben. Möchten Sie die Daten sofort aktualisieren, führen Sie einen Neustart des iQ.Suite Service durch.

Klicken Sie auf **iQ.Suite Reports** und öffnen Sie den gewünschten Report im rechten Fenster mit einem Doppelklick. Im nun erscheinenden neuen Fenster geben Sie den gewünschten Zeitraum für den Report ein. Mit exportieren Sie die Auswertung für den Import in eine andere Anwendung, wobei Sie unter verschiedenen Formaten wählen können.

7 iQ.Suite Crypt

7.1 Übersicht

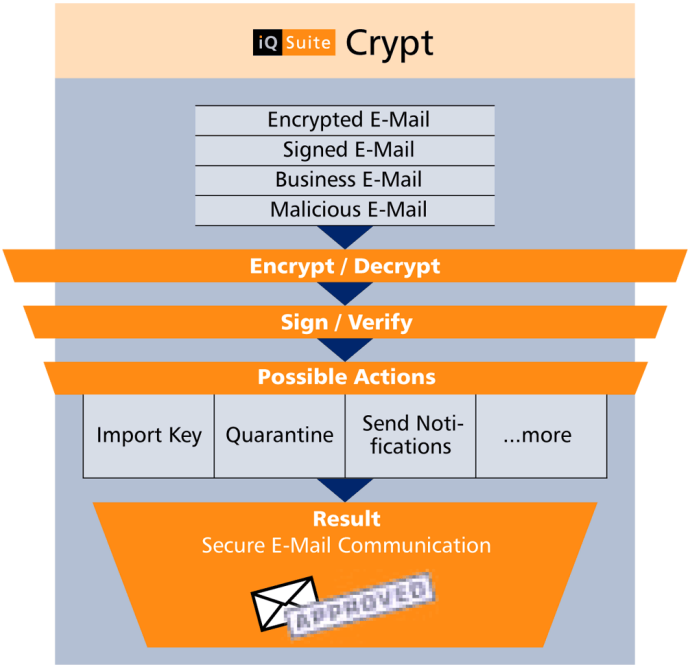
Mit iQ.Suite Crypt verschlüsseln, entschlüsseln, signieren oder verifizieren Sie die E-Mails. Eine Verschlüsselung erfordert auf beiden Seiten ein Verschlüsselungs- und Entschlüsselungswerkzeug (am Server oder alternativ am Client)[15].

Mit iQ.Suite Crypt werden die Mails direkt am Server verschlüsselt und entschlüsselt. Das bedeutet, dass auf dem Weg über das Internet oder andere öffentliche Netze niemand die Mail lesen kann. Die iQ.Suite zieht die Geheimhaltungsgrenze am Serverein- und -ausgang, nicht am Client. Das hat einige Vorteile:

1. Die notwendige Sicherheit gegen Mitleser auf dem Weg durchs Internet ist gewährleistet.
2. Die Viren- und/oder Inhaltsprüfung der E-Mails am Server ist möglich.
3. Die Benutzer genießen höchstmöglichen Komfort, da die gesamte Verschlüsselungsabwicklung am Server durchgeführt wird.
4. Der Installations- und Schulungsaufwand reduziert sich erheblich, da keine Verschlüsselung am Client stattfindet.
5. Die Schlüssel müssen nur einmal am Server eingetragen werden und nicht an jedem Client.

Innerhalb Ihrer Firma wird die E-Mail unverschlüsselt weitergeschickt. Grafisch dargestellt sieht das folgendermaßen aus:

15. Lesen Sie mehr über Kryptographie und Verschlüsselungsverfahren im Crypt Whitepaper, welches Sie auf der Webseite www.group-technologies.com kostenlos herunterladen können.



7.1.1 Jobtypen

- Importieren von PGP-Schlüsseln

  Job: **Crypt Key Import**

- Verschlüsseln oder Signieren von E-Mails

  Job: **Crypt Outbound** mit PGP/GnuPG oder S/MIME

- Entschlüsseln oder Verifizieren von E-Mails

  Job: **Crypt Inbound** mit PGP/GnuPG oder S/MIME

Legen Sie für jeden Crypt-Typ einen separaten Job an! Die Jobtypen lassen sich später nicht mehr ändern.

Die genaue Vorgehensweise für die Job-Einrichtung entnehmen Sie bitte den Jobbeispiel-Beschreibungen, z.B. “PGP Schlüssel importieren - Jobbeispiel” auf Seite 146.

iQ.Suite Crypt kann E-Mails entweder mit PGP/GnuPG, PGP/MIME oder S/MIME ver- und entschlüsseln. Die drei Systeme sind nicht miteinander kompatibel, so dass eine z.B. mit PGP verschlüsselte Nachricht nicht mit S/MIME entschlüsselt werden kann. Es ist aber möglich, alle Verschlüsselungsstandards gleichzeitig auf dem Server zu betreiben.

7.1.2 Quickstart PGP/GnuPG

1. PGP oder GnuPG nach Anleitung installieren. GnuPG finden Sie auch auf der iQ.Suite Installations-CD.
2. Schlüsselpaar nach Anleitung erzeugen.
3. Privaten Schlüssel in den privaten Schlüsselbund einpflegen.
4. Öffentlichen Schlüssel in den öffentlichen Schlüsselbund einpflegen.
5. Öffentlichen Unternehmens-Schlüssel den gewünschten Kommunikationspartnern bekannt geben.
6. Konfigurieren der PGP oder GnuPG Engine, siehe “Beispielkonfiguration GnuPG bzw. PGP” auf Seite 141.
7. Einpflegen der öffentlichen Schlüssel der Kommunikationspartner siehe “Ablauf des Schlüsselimports” auf Seite 146.
8. Optional Einrichten und Aktivieren des Schlüsselimport-Jobs, siehe “PGP Schlüssel importieren - Jobbeispiel” auf Seite 146 und die öffentlichen Schlüssel importieren.
9. Öffentliche Schlüssel der Empfänger unterschreiben.
10. Einrichten des Entschlüsselungs-Jobs, siehe “Ablauf der Entschlüsselung mit PGP oder PGP/MIME” auf Seite 161 und “E-Mails mit PGP/GnuPG entschlüsseln - Jobbeispiel” auf Seite 161.
11. Einrichten des Verschlüsselungs-Jobs, siehe “Ablauf der Verschlüsselung mit PGP oder PGP/MIME” auf Seite 151 und “E-Mails mit PGP/GnuPG verschlüsseln - Jobbeispiel” auf Seite 151.

7.1.3 Quickstart S/MIME

1. Erzeugen eines X.509 Zertifikats als Root-Zertifikat (z.B. **root.pfx**) mit iQ.Suite Trust bzw. einer Zertifikatsverwaltungssoftware. Zertifikate können auch bei einem Trustcenter erworben werden.
2. Erzeugen eines Unternehmens-Zertifikats (z.B. **company.pfx**) aus dem Root-Zertifikat.
3. Ablegen einer Kopie des Original-Root-Zertifikats an einen sicheren Ort.
4. Kopieren der beiden Zertifikate in ein SMIME-Verzeichnis innerhalb von **GrpData**, z.B.: `...\GrpData\SMIME`
5. Optional LDAP: Anlegen der Empfängerzertifikate (öffentliche Schlüssel der Kommunikationspartner) im LDAP. Sie müssen erreichbar und mittels Benutzernamen und E-Mail-Adresse identifizierbar sein.
6. Konfigurieren der S/MIME Engine, siehe “Beispielkonfiguration S/MIME” auf Seite 168.
7. Einrichten des Entschlüsselungs-Jobs, siehe “Ablauf der Entschlüsselung mit S/MIME” auf Seite 181 und “E-Mails mit S/MIME entschlüsseln - Jobbeispiel” auf Seite 181.
8. Einrichten des Verschlüsselungs-Jobs, siehe “Ablauf der Verschlüsselung mit S/MIME” auf Seite 172 und “E-Mails mit S/MIME verschlüsseln - Jobbeispiel” auf Seite 173.

7.2 PGP/GnuPG - Allgemeines

Bei PGP (Pretty Good Privacy) wird die Nachricht vom Absender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und an ihn versendet. Nur der Empfänger kann die für ihn bestimmte Nachricht mit seinem privaten Schlüssel entschlüsseln. Im Gegensatz zu der symmetrischen Verschlüsselungstechnik per Passwort werden keine "abhörsicheren Kanäle" gebraucht, durch die zwischen Sender und Empfänger die Schlüssel ausgetauscht werden.

Installieren Sie PGP oder GnuPG (GNU Privacy Guard - Alternative zu PGP) auf dem Server, so dass Crypt damit arbeiten kann. Informationen über PGP und ausführliche Dokumentationen finden Sie in vielen Sprachen auf der internationalen PGP Homepage unter

http://www.pgpi.org/ (für GnuPG unter http://www.gnupg.org/)

In PGP erzeugen Sie sich ein Schlüsselpaar, bestehend aus dem öffentlichen Schlüssel (Public Key) und dem privaten oder geheimen Schlüssel (Secret- oder Private Key). Der öffentliche Schlüssel wird bekannt gemacht, so dass jeder potenzielle Absender ihn benutzen kann. Der private Schlüssel wird nicht herausgegeben und muss sicher aufgehoben werden.

7.2.1 PGP

Der Mailversand mit PGP bzw. GnuPG wird folgendermaßen durchgeführt:

Der Client sendet eine E-Mail ab. Crypt ermittelt auf dem Server die Schlüssel für alle Empfänger. Crypt ruft PGP auf und PGP verschlüsselt alle Nachrichtentexte und Anhänge (auf Dateibasis). Die Originale werden anschließend durch die verschlüsselten ausgetauscht. Sobald der Austausch vollendet ist, erfolgt die Mailfreigabe zum Versand.

Für die Entschlüsselung der E-Mails mit Crypt legen Sie fest, für welche Absender eine Entschlüsselung gewünscht wird. Das können alle Internetabsender oder einzelne Benutzer sein, die Sie in den Adresseinstellungen eintragen.

Die Ankunft einer E-Mail wird folgendermaßen gehandhabt:

Die verschlüsselte Mail trifft ein. Crypt prüft alle Anhänge. Anschließend prüft Crypt auf verschlüsselten Nachrichtentext, indem unter Anderem der Standardtextstring von PGP
-----BEGIN PGP MESSAGE-----
gesucht wird. Sobald z.B. dieser String gefunden wurde, heißt das, dass der Nachrichtentext verschlüsselt wurde. Jetzt wird mit einem Private Key des Empfängers der Nachrichtentext und Anhang entschlüsselt, die verschlüsselten Teile durch die entschlüsselten ersetzt und die Mail für die Weitergabe zum Client freigegeben. Die Entschlüsselung funktioniert mit einem Passwort, das für alle privaten Schlüssel im Schlüsselbund identisch sein muss. Das Passwort wird von Crypt an PGP übergeben, damit der Private Key benutzt werden kann.

7.2.2 PGP/MIME

iQ.Suite Crypt unterstützt die Ver- und Entschlüsselung mit PGP/MIME.

PGP/MIME ist eine Weiterentwicklung des ersten PGP/Inline Verfahrens, wurde 1996 in RFC 2015 erstmalig definiert und in 2001 überarbeitet in RFC 3156 fest-

gehalten. PGP/MIME verschlüsselt mit dem gleichen Format wie S/MIME, aber mit der Technik von PGP die Mail als Ganzes und nicht in einzelnen Teilen. Der Content Type der Mail ist **multipart encrypted** (oder **multipart signed**). Im Gegensatz zur normalen PGP-Verschlüsselung gehen die Formatinformationen oder Nicht-Ascii-Zeichen wie Umlaute nicht verloren, wenn diese Verschlüsselungsmethode verwendet wird. Auch ist die PGP-Signatur vom Nachrichtentext getrennt im Anhang zu finden, was den Lesefluss und das Antworten erleichtert und insgesamt weniger fehleranfällig ist.

PGP/MIME wird allerdings von einigen Clients noch nicht unterstützt.

7.3 Vorbereitungen für PGP

Wenn Sie E-Mails mit Crypt und PGP/GnuPG verschlüsseln bzw. entschlüsseln wollen, führen Sie folgende Schritte durch:

1. Installieren Sie PGP oder GnuPG auf dem Server. Beachten Sie die Installationsanleitung von PGP/GnuPG.
2. Konfigurieren Sie die **Crypt Engine** für PGP bzw. GnuPG unter **Basis-Konfiguration --> Utility-Einstellungen** der iQ.Suite.
3. Importieren Sie die öffentlichen Schlüssel der Empfänger in den PGP-Schlüsselbund. Dazu können Sie den automatischen Import-Job der iQ.Suite benutzen. Unterschreiben Sie die Schlüssel.
4. Konfigurieren und aktivieren Sie den entsprechenden Crypt-Job.

Es ist wichtig, dass Sie nach dem Import in den PGP-Schlüsselbund die öffentlichen Schlüssel **unterschreiben** und/oder **vertrauen**, ansonsten sind sie nicht verwendbar!

7.4 Konfiguration der PGP bzw. GnuPG Crypt Engine

Wenn Sie PGP oder GnuPG verwenden, achten Sie bitte darauf, welche Version Sie installiert haben. Für die GnuPG Version ab 1.2.x und die PGP-Version 6.5.8 sind die **Crypt Engines** vorkonfiguriert. Das gilt für alle Einstellungen inkl. der Variablen. Andere Versionen von GnuPG oder PGP konfigurieren Sie folgendermaßen:

1. Kopieren Sie die vorkonfigurierte **GnuPG** bzw. **PGP Engine** mit der rechten Maustaste: **Alle Tasks** --> **Duplizieren.**
2. Öffnen Sie die Kopie mit einem Doppelklick.
3. Geben Sie der neuen Engine einen sprechenden Namen, der möglichst die Versionsnummer enthalten sollte.
4. Ändern Sie die Parameter und die Variablen für Ihre Version ab. Nehmen Sie dafür Ihre PGP bzw. GnuPG Dokumentation zur Hand.
5. Klicken Sie **OK**, um die Konfiguration zu speichern.

Sobald die neue PGP bzw. GnuPG Engine angelegt ist, steht sie in allen Jobs zur Verfügung.

7.4.1 Beispielkonfiguration GnuPG bzw. PGP

Als Beispiel wird hier die Konfiguration der **GnuPG** Crypt Engine dargestellt.

Öffnen Sie **Basis-Konfiguration --> Utility-Einstellungen** und klicken Sie auf **Crypt Engines**. Wählen Sie mit einem Doppelklick **GnuPG** aus oder klicken Sie mit der rechten Maustaste auf **Eigenschaften**.

7.4.1.1 Allgemeine Einstellungen

- **GROUP Crypt Interface:**

  Das ist die DLL-Datei, die die Verbindung der iQ.Suite zur **GnuPG Engine** herstellt. Dieser Eintrag darf nicht geändert werden!

- **PGP .exe Datei:**

  Geben Sie hier die PGP .exe Datei mit vollständigem Pfad ein. Beispiel:

  c:\program files\crypt\gnupg\gpg.exe

- **Zeitüberschreitung:**

  Geben Sie die Anzahl der Sekunden an, nach der ein Versuch, die Verbindung zur Crypt Engine herzustellen, abgebrochen wird (wenn die Verbindung bis dahin noch nicht aufgebaut sein sollte). Berücksichtigen Sie bei der Zeitangabe die Performance Ihres Servers.

- **PGP Verzeichnis:**

  Geben Sie hier den vollständigen Pfad zum PGP Verzeichnis ein (Home-Dir). Beispiel:

  c:\program files\crypt\gnupg

- **Öffentl. Schlüsselbund:**

  Geben Sie hier den vollständigen Pfad zu der Datei ein, in der sich die öffentlichen PGP Schlüssel befinden. Beispiel:

  `c:\program files\crypt\gnupg\pubring.gpg`

- **Privater Schlüsselbund:**

  Geben Sie hier den vollständigen Pfad zu der Datei ein, in der sich die privaten PGP Schlüssel befinden. Beispiel:

  `c:\program files\crypt\gnupg\secring.gpg`

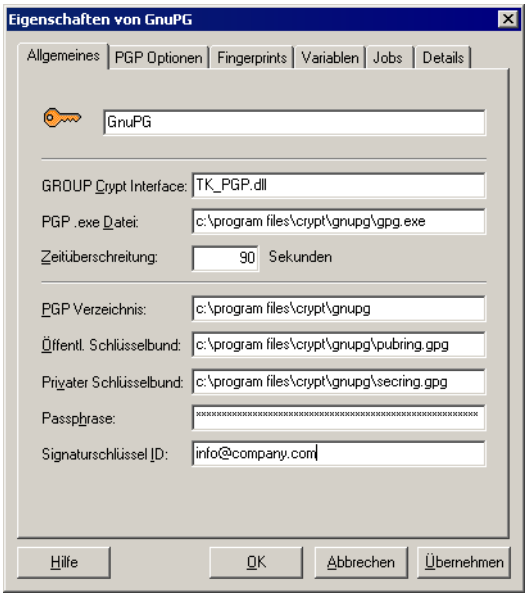
- **Passphrase:**

  In diesem Feld geben Sie die Passphrase für den privaten Schlüsselbund ein. Die Passphrase darf kein Leerzeichen enthalten.

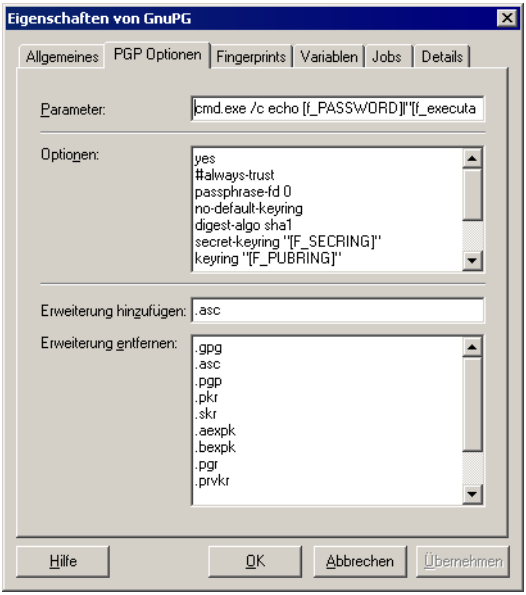
- **Signaturschlüssel ID:**

  Dieses Feld enthält die Schlüsselidentifikation des (privaten) Unternehmens-Schlüssels, der immer zum Signieren verwendet werden soll. Beispiel: *info@company.com*

Fertig konfiguriert könnte diese Registerkarte so aussehen:



7.4.1.2 PGP Optionen einrichten



- **Parameter:**

  Die hier eingetragenen Parameter gelten für die GnuPG Version 1.2.x. In der PGP Konfiguration gelten die Parameter für die PGP Version 6.5.8. Wenn eine andere Version von PGP oder GnuPG installiert worden ist, müssen diese Parameter ggf. geändert werden. Wenden Sie sich in einem solchen Fall bitte an unseren Support.

- **Optionen:**

  Für die hier eingetragenen Optionen gilt das Gleiche wie für die Parameter.

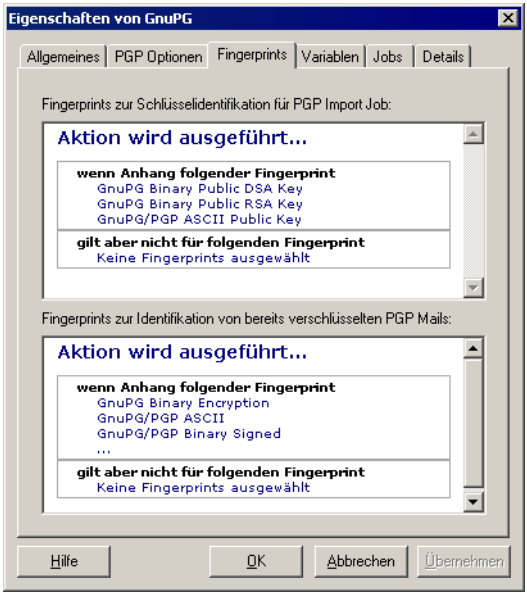
- **Erweiterung hinzufügen:**

  Diese Dateierweiterung (Extension) wird nach der Verschlüsselung mit PGP oder GnuPG jedem einzelnen verschlüsselten Mailabschnitt (Ausnahme: der Nachrichtentext) angehängt und danach versendet. Diese Erweiterungen werden nur bei der Crypt Methode PGP (nicht bei der Methode PGP/MIME) verwendet. Die Crypt Methode wird im Job eingetragen.

Erweiterung entfernen:

Diese Dateierweiterungen (Extension) werden bei der Entschlüsselung wieder von den einzelnen verschlüsselten Mailabschnitten entfernt (abgeschnitten - Ausnahme: der Nachrichtentext), wenn sie eine solche Erweiterung besitzen. Alle hier eingetragenen Erweiterungen werden normalerweise für die PGP-Verschlüsselung verwendet und iQ.Suite Crypt geht davon aus, dass diese Mails die Erweiterung bei einer Verschlüsselung erhalten haben. Die Erweiterungen werden nur bei der Crypt Methode PGP (nicht bei der Methode PGP/MIME) verwendet (im Job einzutragen).

7.4.1.3 Fingerprints hinzufügen oder entfernen



Die Fingerprints im oberen Teil der Registerkarte identifizieren die zu importierenden PGP-Schlüssel. Sobald ein Mail-Abschnitt mit einem hier definierten Fingerprint eingeht, erkennt der Schlüsselimport-Job, dass es sich um einen PGP-Schlüssel handeln muss.

Die Fingerprints im unteren Teil identifizieren die bereits verschlüsselten PGP-Mails, die bereits am Client PGP-verschlüsselt und/oder -signiert worden sind und am Server für den Ausgang verarbeitet werden. Für diese Mails ist im Crypt

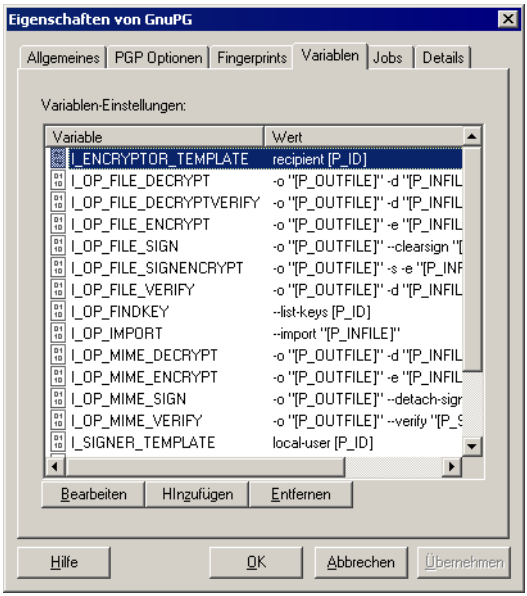
Job eine Ausnahmebehandlung möglich. Die Fingerprints gelten nur für die Crypt Methode PGP, nicht für PGP/MIME.

Alle bekannten Fingerprints zur Identifikation von PGP-Schlüsseln und von verschlüsselten PGP-Mails sind vorkonfiguriert.

Nähere Informationen über Fingerprints entnehmen Sie dem Kapitel “Fingerprints konfigurieren” auf Seite 243.

7.4.1.4 Variablen definieren

Diese Variablen gelten für die GnuPG Version 1.2.x. Die Konfiguration von PGP enthält die Variablen für die PGP Version 6.5.8. Wenn eine andere Version von PGP oder GnuPG installiert worden ist, müssen diese Variablen ggf. geändert werden. Wenden Sie sich in einem solchen Fall bitte an unseren Support.



Klicken Sie **Hinzufügen**, um eine Variable einzufügen bzw. **Bearbeiten**, um eine Variable abzuändern.

7.4.1.5 Jobs überprüfen

Die Registerkarte **Jobs** zeigt, in welchen Jobs die GnuPG Crypt Engine verwendet wird.

7.4.1.6 Details

Die Eingabe der Job Details wird wie in der Beschreibung zu "Details zum Job eingeben" auf Seite 233 durchgeführt.

7.5 Automatischer Schlüsselimport mit PGP/GnuPG

Mit iQ.Suite Crypt ist es möglich, die öffentlichen Schlüssel von Kommunikationspartnern, die mit der verschlüsselten Mail zusammen ihren öffentlichen Schlüssel versenden, automatisch in den Schlüsselbund zu importieren.

7.5.1 Voraussetzungen

Dieses Szenario und die angegebenen Jobs für GnuPG dienen als Beispiel. Der automatische Import ist analog auch mit PGP anwendbar.

- Installiertes PGP oder GnuPG mit den zwei Schlüsselbunden.
- Die Konfiguration der GnuPG bzw. PGP Engine ist abgeschlossen.
- Der Crypt-Job **Schlüsselimport mit GnuPG** (oder ein Job Schlüsselimport mit PGP) ist aktiv und hat eine niedrigere Priorität in der Jobkette als der Entschlüsselungsjob.

7.5.2 Ablauf des Schlüsselimports

1. Der in der Mail enthaltene öffentliche Schlüssel des Senders wird aus der Mail herauskopiert.
2. Der öffentliche Schlüssel wird in den Schlüsselbund importiert.
3. Die Mail wird dem Empfänger zugestellt.
4. Der importierte Schlüssel muss anschließend mit einem privaten Schlüssel unterschrieben (und/oder „vertraut") werden. Den importierten Schlüsseln wird nicht automatisch vertraut.

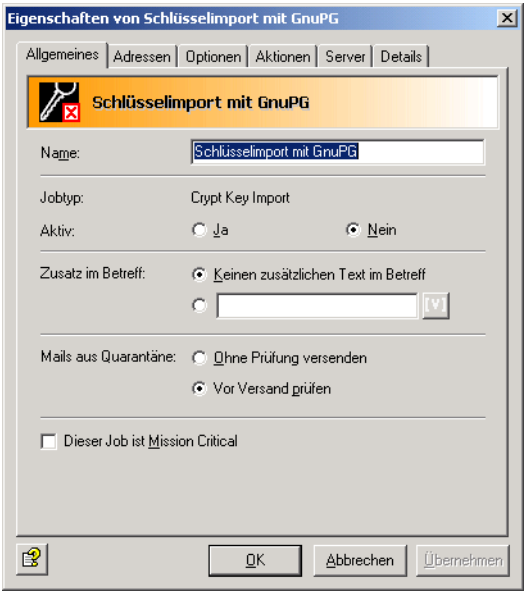
Danach können Mails an diesen Absender verschlüsselt werden.

7.5.3 PGP Schlüssel importieren - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie den Job **Schlüsselimport mit GnuPG**. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

7.5.3.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Dieser Job fügt keinen **Zusatz im Betreff** ein, da dieser Job keine Mails an irgendeinen Empfänger weiterschickt. Es wird nur der Schlüssel aus der Mail ausgelesen und in den öffentlichen Schlüsselbund importiert.

Dieser Job bearbeitet auch diejenigen Mails, die aus der **Quarantäne** wieder versendet werden. Die **Sende-Option** beim Versand aus der Quarantäne ist Job-übergreifend und hat Priorität. Wenn Sie eine Mail also mit der Quarantäne-Sende-Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die **Sende-Option** deshalb auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**.

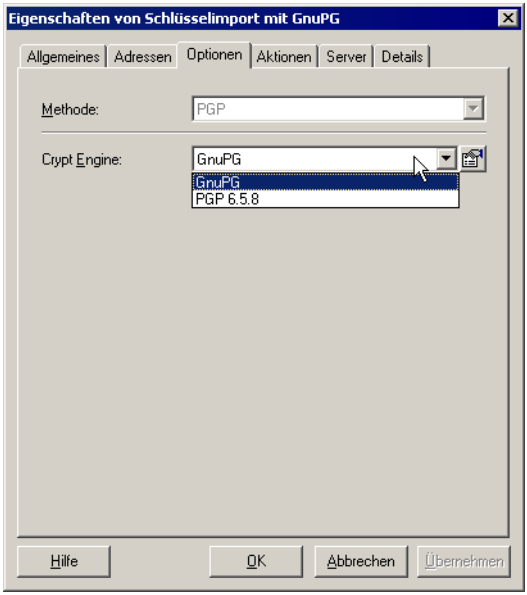
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

7.5.3.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

7.5.3.3 Optionen auswählen - Crypt Engine

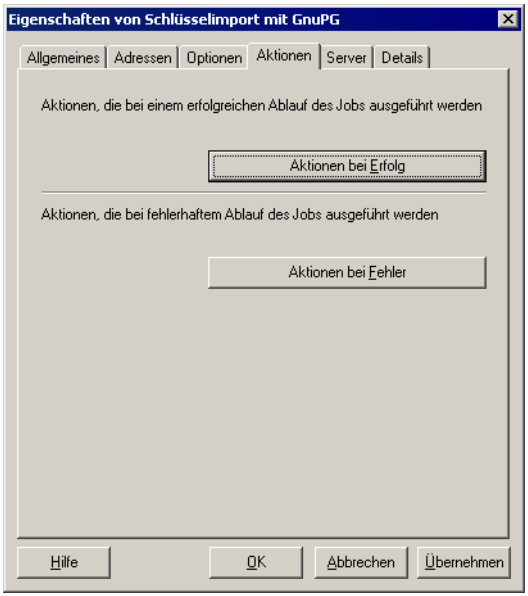
In der Registerkarte **Optionen** wählen Sie die **Crypt Engine**. Ein Schlüsselimport ist nur mit **PGP** möglich, deshalb ist die Verschlüsselungsmethode bereits auf PGP voreingestellt und lässt sich auch nicht ändern. Für die Crypt Engine haben Sie die Wahl zwischen PGP und **GnuPG**.



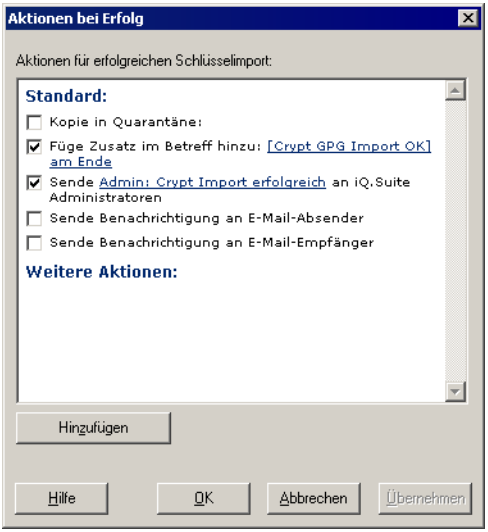
Sollten Sie einen PGP Schlüsselimport durchführen wollen, achten Sie bitte auf die richtige Konfiguration Ihrer PGP-Version. Die vorkonfigurierte PGP-Version ist 6.5.8. Wenn Sie eine andere Version verwenden, so legen Sie diese neu in der **Basis-Konfiguration --> Utility-Einstellungen** unter **Crypt Engines** an. Anschließend steht Ihnen diese Version hier im Pull-Down-Menü zur Verfügung. Wenn Sie auf die Eigenschaften-Schaltfläche klicken, können Sie die Konfiguration der hier gewählten Crypt Engine aufrufen. Lesen Sie bitte das Kapitel "Konfiguration der PGP bzw. GnuPG Crypt Engine" auf Seite 140.

7.5.3.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Schlüsselimport erfolgreich durchgeführt worden ist und welche Aktionen durchgeführt werden, wenn ein Fehler aufgetreten ist.



Klicken Sie auf **Aktionen bei Erfolg**. Hier sind folgende Aktionen definiert:



Als Aktion wird eine Benachrichtigung an den Administrator mit dem Betreff **Crypt GPG Import OK** versandt. Die Benachrichtigungsvorlage ist **Admin: Crypt Import erfolgreich**. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt. Diese können individuell über die HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[16]. In gleicher Form definieren Sie die **Aktionen bei Fehler**: Eine Benachrichtigung wird an den Administrator versandt und die Mail außerdem in die Quarantäne gestellt.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

7.5.3.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

16. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100

7.6 Verschlüsseln mit PGP/GnuPG

7.6.1 Voraussetzungen

Dieses Szenario und die angegebenen Jobs für GnuPG dienen als Beispiel. Die Verschlüsselung ist analog auch mit PGP anwendbar.

- Installiertes PGP oder GnuPG mit den zwei Schlüsselbunden.
- Der öffentliche Schlüssel des Empfängers ist im Schlüsselbund vorhanden und durch einen privaten Schlüssel signiert.
- Die Konfiguration der GnuPG Engine ist abgeschlossen.
- Ein Crypt-Job **Verschlüsseln/signieren mit GnuPG** (oder **PGP**) ist aktiv.
- Im entsprechenden Crypt-Job **Verschlüsseln/signieren mit GnuPG** (oder **PGP**) sind die Adressen für die Empfänger konfiguriert. Gegebenenfalls werden mehrere Jobs erstellt und aktiviert.

7.6.2 Ablauf der Verschlüsselung mit PGP oder PGP/MIME

1. Der Benutzer versendet seine E-Mail über seinen Client, wie er es normalerweise gewohnt ist.
2. Auf dem Server holt sich Crypt den öffentlichen Schlüssel für die Empfänger der E-Mail aus dem Schlüsselbund vom GnuPG bzw. PGP.
3. Die Mail wird verschlüsselt. Bei PGP werden alle Einzelteile einer Mail verschlüsselt (Achtung: Formatinformationen und eingebettete Bilder gehen verloren), bei PGP/MIME wird eine Mail im Ganzen verschlüsselt (die Formatinformationen bleiben erhalten).
4. Die Mail wird den Empfängern zugestellt.

7.6.3 E-Mails mit PGP/GnuPG verschlüsseln - Jobbeispiel

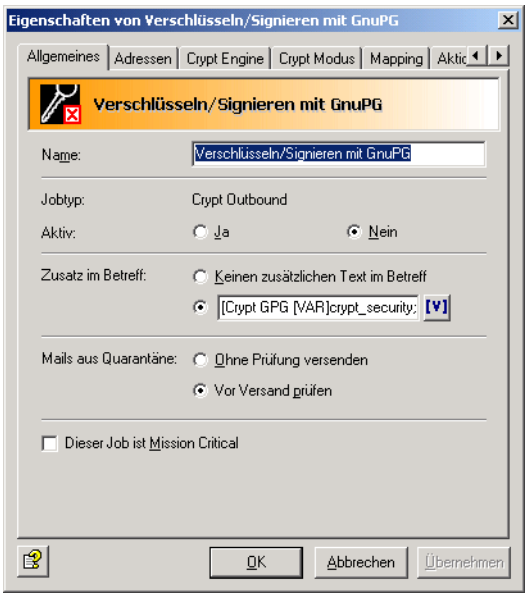
Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie zwei Jobs für die Verschlüsselung.

- Verschlüsseln/signieren mit GnuPG
- Verschlüsseln/signieren mit PGP

Als Beispiel wird hier **Verschlüsseln/signieren mit GnuPG** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

7.6.3.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist mit einer Variablen (siehe “Liste der Benachrichtigungs-variablen” auf Seite 101) vordefiniert. Dieser Zusatz wird in den Betreff jeder Mail eingefügt, die erfolgreich verschlüsselt worden ist.

Dieser Job bearbeitet auch diejenigen Mails, die aus der **Quarantäne** wieder versendet werden. Die **Sende-Option** beim Versand aus der Quarantäne ist Job-übergreifend und hat Priorität. Wenn Sie eine Mail also mit der Quarantäne-Sende-Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die **Sende-Option** deshalb auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**.

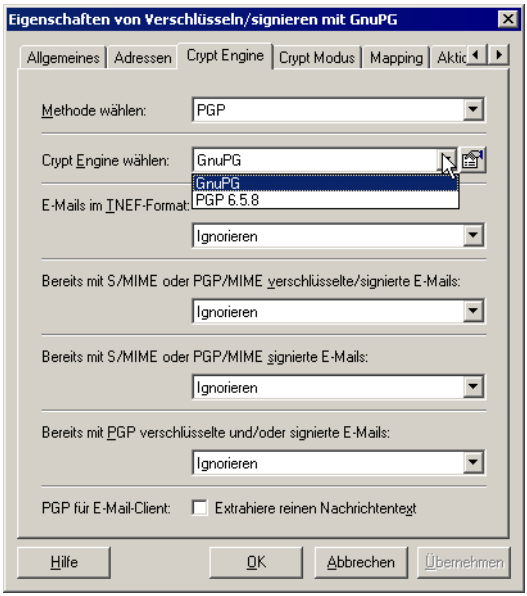
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

7.6.3.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

7.6.3.3 Crypt Engine auswählen - Verschlüsselungsmethode

In der Registerkarte **Crypt Engine** stellen Sie ein, welche Verschlüsselungsmethode und dazugehörige Optionen mit diesem Job aufgerufen werden sollen.



Die hier gewählte Verschlüsselungs**methode** ist **PGP**. Die Crypt Engine ist **GnuPG**. Anschließend können Sie festlegen, wie Sie die Mail-Sonderfälle behandeln wollen. Dabei haben Sie folgende Möglichkeiten:

- **Ignorieren**

  Diese Mail wird nicht weiter von diesem Job bearbeitet, sondern an den nächsten Job weitergereicht. Die Mail wird nicht verschlüsselt oder signiert.

- **Aktionen ausführen**

  Die definierten Aktionen auf der Registerkarte **Aktionen** werden ausgeführt.

- **Verarbeiten**

  Der Job behandelt die Mail genauso wie andere, die nicht unter diese Rubrik fallen.

Die einzelnen Sonderfälle:

- **E-Mails im TNEF-Format**

  Das Outlook-Format TNEF (**T**ransport **N**eutral **E**ncapsulation **F**ormat) kann nicht von iQ.Suite Crypt bearbeitet werden. Das TNEF-Format wird von Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine E-Mail sendet. Bei der Kommunikation über das Internet bzw. bei der Verwendung von anderen E-Mail Programmen wird dieses Format nicht verwendet. Möchten Sie iQ.Suite Crypt auch für die interne Verschlüsselung nutzen, können Sie für TNEF-Mails die Optionen **Ignorieren** oder **Aktionen ausführen** wählen.

- **Bereits mit S/MIME oder PGP/MIME verschlüsselte/signierte E-Mails**

  E-Mails, die bereits verschlüsselt (und signiert) am Server ankommen, sind vom Client, also vom Benutzer verschlüsselt worden. Legen Sie in den E-Mail-Richtlinien Ihres Unternehmens fest, wie Sie solche Fälle behandeln wollen. Diese Einstellung gilt nur für Mails, die S/MIME oder PGP/MIME verschlüsselt oder verschlüsselt und signiert am Server eintreffen.

- **Bereits mit S/MIME oder PGP/MIME signierte E-Mails**

  Auch E-Mails, die bereits vom Benutzer signiert am Server ankommen, können Sie anders behandeln. Diese Einstellung gilt ebenfalls nur für Mails, die mit S/MIME oder PGP/MIME nur signiert und nicht verschlüsselt am Server ankommen.

- **Bereits mit PGP verschlüsselte oder signierte E-Mails**

  Bei PGP/MIME und S/MIME lässt sich an der Struktur und den Kopfzeilen (Header) der E-Mail erkennen, ob sie verschlüsselt oder signiert ist. Bei einer Verschlüsselung mit PGP werden nur die Inhalte der **einzelnen Mail-Abschnitte** durch den verschlüsselten Teil ersetzt, nicht die gesamte E-Mail. Die Struktur ändert sich nicht. Um also erkennen zu können, ob eine Mail ganz oder in Teilen durch PGP bearbeitet (verschlüsselt oder signiert oder beides) wurde, werden die in der Konfiguration angegebenen Fingerprints auf alle Einzelteile einer Mail (Nachrichtentext und Anhänge) angewendet. Die PGP-Fingerprints für einzelne E-Mail-Abschnitte definieren Sie in der Konfiguration der PGP bzw. GnuPG Crypt Engine.

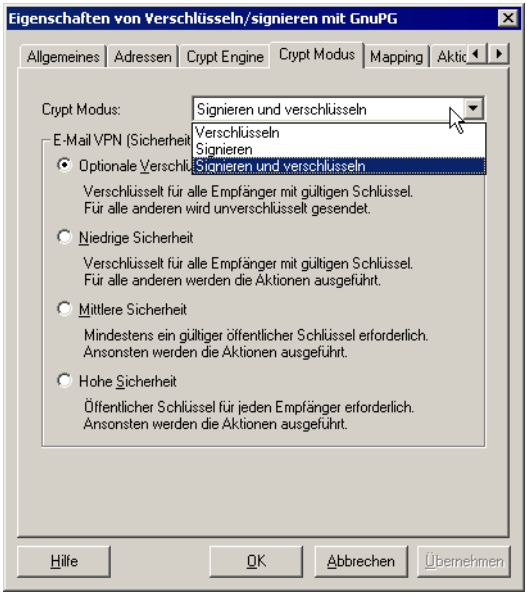
- **Extrahiere reinen Nachrichtentext**

  PGP-Client-Applikationen oder -Plugins können gewöhnlich kein HTML rendern. Da Crypt die einzelnen Mail-Abschnitte getrennt voneinander verschlüsselt, bleiben die Formatinformationen im HTML-Nachrichtentext erhalten. Will der Empfänger nun mit seinem PGP-Client den Inhalt der Mail anschauen, bekommt er den Inhalt zusammen mit dem HTML-Code zu sehen. Um zu verhindern, dass dem Empfänger die verwirrenden HTML-Tags angezeigt werden, kann Crypt das HTML entfernen und nur den reinen Nachrichtentext übertragen. Diese Option sollten Sie aktivieren, sobald Sie verschlüsselte E-Mails direkt an E-Mail-Clients senden. Bei der Korrespondenz mit einem Kommunikationspartner, der ebenfalls Crypt am Server einsetzt, werden die HTML-Mails korrekt dargestellt. Schalten Sie in einem solchen Fall die Option aus.

Bei Mails, die als „nur HTML“ versendet werden, wird der HTML-Teil beibehalten. Das „nur HTML“-Format wird von einigen E-Mail-Clients angeboten.

7.6.3.4 Crypt Modus auswählen - Verschlüsselungsmodus - VPN

In der Registerkarte **Crypt Modus** stellen Sie ein, welcher Verschlüsselungsmodus und welche **Sicherheitseinstellungen** (VPN Kanal) mit diesem Job aufgerufen werden sollen.



Der hier gewählte **Crypt Modus** ist **Signieren und verschlüsseln**. Die Möglichkeiten sind:

- **Signieren und verschlüsseln**

  Die Mail wird gleichzeitig signiert und verschlüsselt.

- **Verschlüsseln**

  Die Mail wird nur verschlüsselt und nicht signiert.

- **Signieren**

  Die Mail wird nur signiert und nicht verschlüsselt.

Die einzelnen Optionsmöglichkeiten zeigen die möglichen **Sicherheitseinstellungen** für ausgehende E-Mails (**VPN** Kanäle). Alle Optionen gelten nur für die Verschlüsselung, da das Signieren mit dem privaten Schlüssel erfolgt, bei Fehlen dieses Schlüssels sofort fehlschlägt und die definierten **Aktionen** durchgeführt werden.

Optionale Verschlüsselung

Die Mails werden mit den vorhandenen öffentlichen Schlüsseln verschlüsselt. Allen Empfängern, für die kein gültiger Schlüssel vorliegt, erhalten die Mail unverschlüsselt.

Niedrige Sicherheit

Die Mails werden mit den vorhandenen öffentlichen Schlüsseln verschlüsselt. Die Adressaten mit gültigem Schlüssel erhalten die Mail verschlüsselt. Für alle Empfänger ohne gültigen Schlüssel werden die auf der Registerkarte **Aktionen** definierten Maßnahmen durchgeführt.

Mittlere Sicherheit

Die Mails werden nur dann mit den vorhandenen öffentlichen Schlüsseln verschlüsselt, wenn **mindestens ein gültiger Schlüssel** vorliegt. Alle Adressaten erhalten die Mail verschlüsselt. Die Adressaten mit gültigem Schlüssel können die Mail mit ihrem privaten Schlüssel öffnen. Alle Empfänger ohne gültigen Schlüssel werden also die verschlüsselte Mail nicht öffnen können, da sie keine passenden privaten Schlüssel zu den verwendeten öffentlichen Schlüsseln besitzen. Die auf der Registerkarte **Aktionen** definierten Maßnahmen werden nur durchgeführt, wenn überhaupt kein gültiger Schlüssel vorhanden ist.

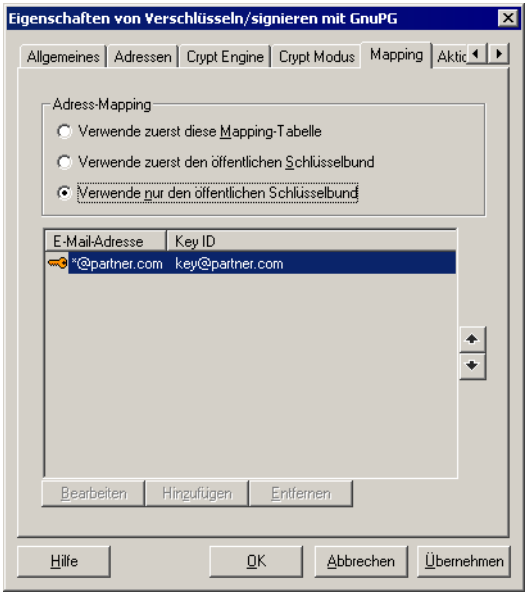
Hohe Sicherheit

Die Mails werden nur dann mit den vorhandenen öffentlichen Schlüsseln verschlüsselt, wenn **für alle Adressaten ein gültiger Schlüssel** vorliegt. Die auf der Registerkarte **Aktionen** definierten Maßnahmen treten sofort in Kraft, wenn nur ein einziger Schlüssel ungültig ist oder fehlt.

Ein Job kommt nur für diejenigen Adressaten zur Ausführung, die Sie in der Registerkarte **Adressen** festgelegt haben. Wenn Sie dort nur die Kommunikationspartner mit einem gültigen öffentlichen Schlüssel eintragen, können Sie mit der Auswahl einer hohen Sicherheitseinstellung „abhörsichere“ Kanäle schaffen, ohne dass Fehler wegen fehlender Schlüssel auftreten und die definierten **Aktionen** durchgeführt werden. Legen Sie für jede Sicherheitseinstellung einen Job an, also zwei Jobs, wenn Sie Mails für einige Adressen sehr sicher übertragen wollen und alle anderen Kommunikationspartner nur optional verschlüsselt werden sollen.

7.6.3.5 Mapping auswählen - Key ID-Zuordnung

In der Registerkarte **Mapping** bestimmen Sie die Art des Adressmappings für die Verschlüsselung und erstellen bei Bedarf Ihre eigene Mapping-Tabelle.



Die Voreinstellung ist **Verwende nur den öffentlichen Schlüsselbund**. Die Möglichkeiten sind:

- **Verwende zuerst diese Mapping-Tabelle**

  Die Einträge in der unten stehenden selbst definierten Mapping-Tabelle haben Vorrang vor den Einträgen im öffentlichen Schlüsselbund (public key ring). Wenn in dieser Tabelle eine Key ID eingetragen ist, wird im öffentlichen Schlüsselbund nach dieser Key ID gesucht und der dazu gehörige Schlüssel verwendet. Erst wenn kein passender Eintrag in der Tabelle gefunden worden ist, sucht der Verschlüsselungsjob im öffentlichen Schlüsselbund unter der Empfänger-Adresse als Key ID. Diese Einstellung ist sinnvoll, wenn über sichere VPN Kanäle eine Verschlüsselung mit einem bestimmten Unternehmen verwirklicht werden soll.

- **Verwende zuerst den öffentlichen Schlüsselbund**

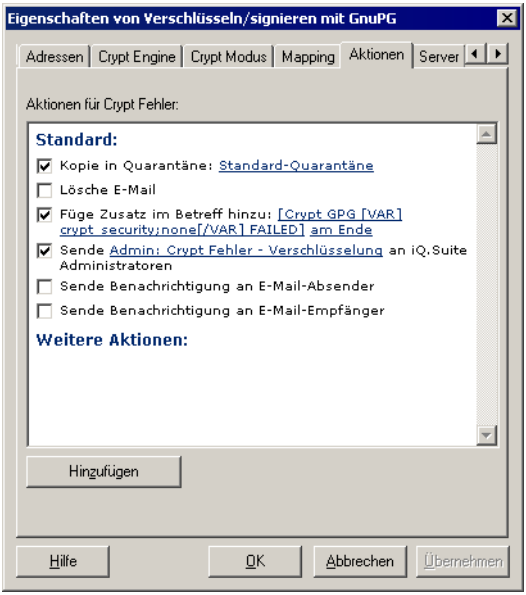
  Die Einträge im öffentlichen Schlüsselbund haben Vorrang vor den Einträgen in der selbst definierten Mapping-Tabelle. Erst wenn kein zur Empfängeradresse passender Eintrag im Schlüsselbund gefunden worden ist, sucht der Job in der unten stehenden Mapping-Tabelle die benötigte Key ID. Beispiel: Mails, die an die Geschäftsleitung gesondert verschlüsselt werden sollen.

- **Verwende nur den öffentlichen Schlüsselbund**

  Die Schlüssel werden ausschließlich anhand der Empfängeradresse im öffentlichen Schlüsselbund gesucht. In diesem Fall wird die Mapping-Tabelle nicht aktiviert; evtl. Einträge bleiben aber erhalten. Diese Einstellung wird verwendet, wenn mit Einzelpersonen kommuniziert wird, die jeweils einen eigenen Schlüssel haben.

7.6.3.6 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn die Verschlüsselung durch den Job fehlgeschlagen ist.



Als Aktion wird eine Kopie in die Quarantäne gestellt. Das beinhaltet, dass die Mail dem Empfänger trotzdem zugestellt wird. Eine Benachrichtigung über die nicht erfolgte Verschlüsselung wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt. Diese können individuell über die HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[17].

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

7.6.3.7 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

17. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100

7.7 Entschlüsseln mit PGP/GnuPG

7.7.1 Voraussetzungen

Dieses Szenario und die angegebenen Jobs für GnuPG dienen als Beispiel. Die Entschlüsselung ist analog auch mit PGP anwendbar.

- Installiertes PGP oder GnuPG mit den zwei Schlüsselbunden.
- Ein passender privater Schlüssel ist im Schlüsselbund vorhanden.
- Die Konfiguration der GnuPG Engine ist abgeschlossen.
- Ein Crypt-Job **Entschlüsseln/Verifizieren mit GnuPG** ist aktiv.
- Im entsprechenden Crypt-Job **Entschlüsseln/Verifizieren mit GnuPG** sind die Adressen für die Empfänger konfiguriert. Gegebenenfalls werden mehrere Jobs erstellt und aktiviert.

7.7.2 Ablauf der Entschlüsselung mit PGP oder PGP/MIME

1. Auf dem Server holt sich iQ.Suite Crypt für die eingehende Mail den privaten Schlüssel für diese Mail aus dem Schlüsselbund vom GnuPG bzw. PGP.
2. Die Mail wird entschlüsselt. Bei PGP werden die einzelnen verschlüsselten Teile der Mail entschlüsselt, bei PGP/MIME wird die Mail im Ganzen entschlüsselt.
3. Die Mail wird dem Empfänger zugestellt.
4. Der Benutzer empfängt seine E-Mail über seinen Client, wie er es normalerweise gewohnt ist, ohne etwas von der ursprünglichen Verschlüsselung zu bemerken.

7.7.3 E-Mails mit PGP/GnuPG entschlüsseln - Jobbeispiel

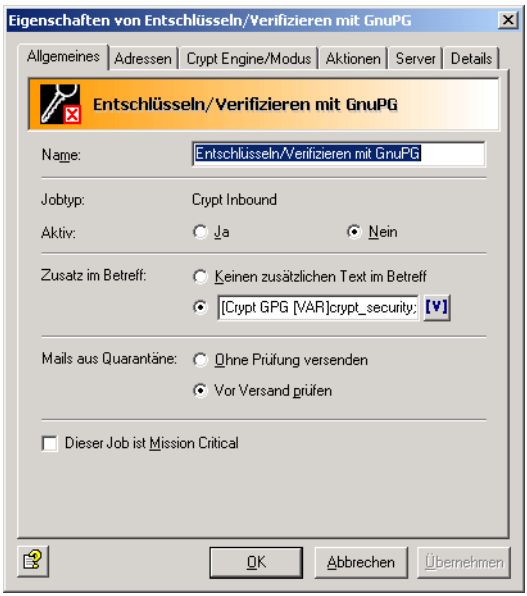
Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie zwei Jobs für die Verschlüsselung.

- Entschlüsseln/Verifizieren mit GnuPG
- Entschlüsseln/Verifizieren mit PGP

Als Beispiel wird hier **Entschlüsseln/Verifizieren mit GnuPG** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

7.7.3.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist mit einer Variablen (siehe “Liste der Benachrichtigungs-variablen” auf Seite 101) vordefiniert. Dieser Zusatz wird in den Betreff jeder Mail eingefügt, die erfolgreich entschlüsselt worden ist.

Dieser Job bearbeitet auch diejenigen Mails, die aus der **Quarantäne** wieder versendet werden. Die **Sende-Option** beim Versand aus der Quarantäne ist Job-übergreifend und hat Priorität. Wenn Sie eine Mail also mit der Quarantäne-Sende-Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die **Sende-Option** deshalb auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**.

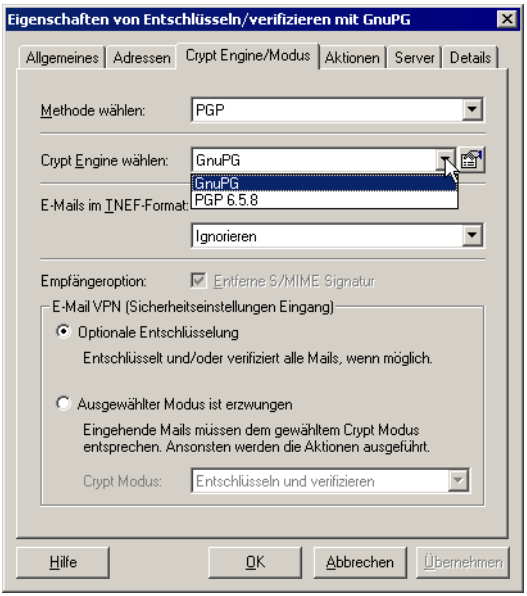
Näheres zum erneuten Versand aus der Quarantäne finden Sie in "Aus Quarantäne senden" auf Seite 130. Die Option **Mission Critical** finden Sie unter **Dieser Job ist Mission Critical** näher beschrieben.

7.7.3.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in "Adresslisten" auf Seite 90.

7.7.3.3 Crypt Engine/Modus auswählen - Methode

In der Registerkarte **Crypt Engine/Modus** stellen Sie ein, welche Entschlüsselungsmethode und welche Sicherheitseinstellungen mit diesem Job aufgerufen werden sollen. Außerdem können Sie hier Zusatzoptionen einrichten.



Die hier gewählte Entschlüsselungs**methode** ist **PGP**. Die **Crypt Engine** ist **GnuPG**. Anschließend können Sie festlegen, wie Sie den Sonderfall **E-Mails im TNEF-Format** behandeln wollen. Dabei haben Sie folgende Möglichkeiten:

- **Ignorieren**
  Diese Mail wird nicht weiter von diesem Job behandelt, sondern an den nächsten Job weitergereicht.

- **Aktionen ausführen**
  Die definierten Aktionen auf der Registerkarte **Aktionen** werden ausgeführt.

Die einzelnen Optionen:

- **E-Mails im TNEF-Format**
  Das Outlook-Format TNEF (**T**ransport **N**eutral **E**ncapsulation **F**ormat) kann nicht von iQ.Suite Crypt bearbeitet werden. Das TNEF-Format wird von Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine E-Mail sendet. Bei der Kommunikation über das Internet bzw. bei der Verwendung von anderen E-Mail Programmen wird dieses Format nicht verwendet. Möchten Sie iQ.Suite Crypt auch für die interne Verschlüsselung nutzen, können Sie für TNEF-Mails die Optionen **Ignorieren** oder **Aktionen ausführen** wählen.

- **Für Empfänger: Entferne S/MIME Signatur**
  Diese Einstellung ist bei der PGP Entschlüsselung nicht notwendig und nur dann verfügbar, wenn die Entschlüsselungsmethode PGP/MIME oder S/MIME ist. Die Bedeutung dieser Option entnehmen Sie bitte der Beschreibung in “Crypt Engine/Modus auswählen - Methode” auf Seite 183.

Modus und Sicherheitseinstellungen (VPN Kanäle):

Die einzelnen Optionsmöglichkeiten zeigen die möglichen **Sicherheitseinstellungen** für eingehende E-Mails (**VPN** Kanäle). Die Voreinstellung ist **Optionale Entschlüsselung**.

Es gibt für die Entschlüsselung zwei mögliche Sicherheitseinstellungen:

- **Optionale Entschlüsselung**
  Die Mails werden - wenn möglich - mit den vorhandenen privaten Schlüsseln entschlüsselt und die Signatur - wenn möglich - mit den vorhandenen öffentlichen Schlüsseln verifiziert. Sollte eine Mail nicht verschlüsselt oder signiert sein, erhalten die Empfänger die Mails so wie sie sind. Tritt bei der

Entschlüsselung oder Verifizierung ein Fehler auf, z.B. weil der private Schlüssel fehlt oder die Mail verändert wurde und damit nicht verifiziert werden kann, so werden die konfigurierten Aktionen ausgeführt.

- **Ausgewählter Modus ist erzwungen**

  Es werden nur diejenigen eingehenden E-Mails an den Empfänger weitergegeben, die exakt dem ausgewählten Modus im Pull-Down-Menü entsprechen. Wenn Sie also beispielsweise **Verifizieren und entschlüsseln** wählen, dann müssen die eingehenden Mails sowohl signiert als auch verschlüsselt sein. Die Bedingung gilt als nicht erfüllt, wenn die Mail nur verschlüsselt eingeht und nicht signiert ist. Für alle Mails, die dem ausgewählten Modus nicht entsprechen, werden die auf der Registerkarte **Aktionen** definierten Maßnahmen durchgeführt. Sie können folgende Modi auswählen:

  - **Entschlüsseln und verifizieren**

    Die Mail wird gleichzeitig entschlüsselt und verifiziert. Unter diese Bedingung fallen nur diejenigen Mails, die signiert **und** verschlüsselt am Server ankommen.

  - **Entschlüsseln**

    Die Mail wird nur entschlüsselt. Nur signierte oder signierte und verschlüsselte Mails fallen nicht unter diese Bedingung.

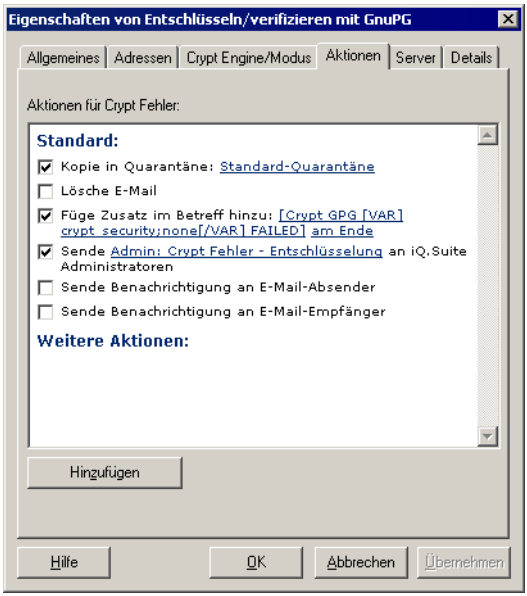
  - **Verifizieren**

    Die Mail wird nur verifiziert. Nur verschlüsselte oder signierte und verschlüsselte Mails fallen nicht unter diese Bedingung.

Ein Job kommt nur für diejenigen Adressaten zur Ausführung, die Sie in der Registerkarte **Adressen** festgelegt haben. Wenn Sie dort nur die Kommunikationspartner eintragen, mit denen Sie beispielsweise vereinbart haben, dass alle E-Mails sowohl signiert als auch verschlüsselt übertragen werden sollen, können Sie mit der Auswahl des erzwungenen Modus „abhörsichere“ Kanäle schaffen, ohne dass Fehler wegen einer Mail im falschen Modus auftreten und die definierten **Aktionen** durchgeführt werden. Legen Sie für jede Sicherheitseinstellung einen Job an, also zwei Jobs, wenn Sie Mails für einige Adressen sehr sicher übertragen wollen und alle anderen Kommunikationspartner nur optional entschlüsselt bzw. verifiziert werden sollen.

7.7.3.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn die Entschlüsselung bzw. Verifizierung durch den Job **fehlgeschlagen** ist.



Als Aktion wird eine Kopie in die Quarantäne gestellt. Das beinhaltet, dass die Mail dem Empfänger trotzdem zugestellt wird. Eine Benachrichtigung über die nicht erfolgte Entschlüsselung wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt. Diese können individuell über die HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[18].

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

7.7.3.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

7.8 S/MIME - Allgemeines

S/MIME ist eine Abkürzung für „Secure MIME“. Um S/MIME-konform zu verschlüsseln oder zu signieren, erwerben Sie Zertifikate bei einem Trustcenter. Falls Sie keine rechtsverbindlichen Zertifikate benötigen, verwenden Sie unser Produkt iQ.Suite Trust, um einfach und schnell Zertifikate zu erstellen. Im Unterschied zu PGP erzeugt sich der Anwender das Schlüsselpaar bei S/MIME nicht selbst, sondern erhält die Schlüssel von der Zertifizierungsstelle. Der Aufbau der Zertifikate ist nach dem X.509-Standard festgelegt[19].

7.8.1 Vorbereitungen für S/MIME

Führen Sie folgende Schritte durch:

1. Erzeugen Sie die X.509 Zertifikate mit iQ.Suite Trust oder einer anderen Zertifikatsverwaltungssoftware:
   a) Ein Root-Zertifikat (auch Aussteller-Zertifikat (z.B. **root.pfx**)) und
   b) ein daraus abgeleitetes Unternehmens-Zertifikat (z.B. **company.pfx**).

18. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100
19. Die S/MIME-Implementierung von iQ.Suite Crypt verwendet als Verschlüsselungsverfahren RC2 mit 128-Bit-Schlüsseln und für den Signatur-Hash SHA1.

2. Kopieren Sie die beiden Dateien in das Verzeichnis **... /GrpData/smime-data**. Es empfiehlt sich, eine Kopie des Root-Zertifikates sicher zu verwahren.
3. Konfigurieren Sie die **Crypt Engine** für S/MIME in der **Basis-Konfiguration --> Utility-Einstellungen** der iQ.Suite. Sollten Sie die Zertifikate der Kommunikationspartner bereits in einem LDAP-Server eingetragen haben, richten Sie den LDAP-Server unter S/MIME-Optionen ein.
4. Konfigurieren und aktivieren Sie den Job **Verschlüsseln/Signieren mit S/MIME** im iQ.Suite Frontend. Stellen Sie den **Crypt Modus** auf der Registerkarte **Crypt Modus** auf **Signieren** ein.
5. Wenn Sie E-Mails mit Crypt und S/MIME **verschlüsseln** oder **entschlüsseln** wollen, konfigurieren und aktivieren Sie den Job **Verschlüsseln/Signieren mit S/MIME** im iQ.Suite Frontend. Stellen Sie aber in diesem Fall den **Crypt Modus** auf der Registerkarte **Crypt Modus** auf **Verschlüsseln** ein.
6. Wenn Sie E-Mails mit Crypt und S/MIME **verschlüsseln/ entschlüsseln** und gleichzeitig **signieren/verifizieren** wollen, stellen Sie den **Crypt Modus** auf der Registerkarte **Crypt Modus** auf **Signieren und verschlüsseln** ein.

7.9 Konfiguration der S/MIME Crypt Engine

Wenn Sie S/MIME zum Verschlüsseln bzw. Signieren verwenden, konfigurieren Sie die S/MIME Crypt Engine.

7.9.1 Beispielkonfiguration S/MIME

Öffnen Sie die **Basis-Konfiguration --> Utility-Einstellungen** und klicken Sie auf **Crypt Engines**. Wählen Sie mit einem Doppelklick **S/MIME** aus oder klicken Sie mit der rechten Maustaste auf **Eigenschaften**.

7.9.1.1 Allgemeine Einstellungen

Für den Standardfall genügt es, wenn Sie in dieser Registerkarte nur noch die Namen Ihrer Zertifikate überprüfen und die Passwörter eintragen.

- **GROUP Crypt Interface:**
  Das ist die DLL-Datei, die die Verbindung der iQ.Suite zur **GnuPG Engine** herstellt. Dieser Eintrag darf nicht geändert werden!

- **Zeitüberschreitung:**

  Geben Sie die Anzahl der Sekunden an, nach der ein Versuch, die Verbindung zur Crypt Engine herzustellen, abgebrochen wird (wenn die Verbindung bis dahin noch nicht aufgebaut sein sollte). Berücksichtigen Sie bei der Zeitangabe die Performance Ihres Servers.

- **Pfad für Zertifikate:**

  Die feste Vorgabe für das S/MIME-Datenverzeichnis, in dem sich unter Anderem die zwei Datenbank-Dateien mit den öffentlichen Zertifikaten befinden, ist der Ordner **...\smimedata,** der unterhalb von **GrpData** angelegt wird. **Ändern Sie diesen Ordnernamen nicht ab!**

- **Root-Zertifikat:**

  Kopieren Sie das Root-Zertifikat (`pfx`-Datei) in den oben genannten Zertifikate-Ordner. Geben Sie den Namen des Zertifikates **inklusive** des Zertifikate-Ordners hier ein. Beispiel:

  `smimedata\root.pfx`

  Sie können diesen Pfad ändern, wenn Ihre Zertifikate in einem anderen Verzeichnis abgelegt werden müssen. Geben Sie in diesem Fall aber den absoluten Pfad des Ordners (Verzeichnis) an. Beispiel:

  `c:\program files\crypt\smime\root.pfx`

- **Unternehmens-Zertifikat:**

  Das Unternehmens-Zertifikat (`pfx`-Datei) wird aus dem Root-Zertifikat erzeugt und muss im gleichen Verzeichnis wie das Root-Zertifikat liegen. Beispiel:

  `smimedata\company.pfx`

  Sollten Sie für das Root-Zertifikat einen absoluten Pfad mit einem anderen Ordner als **smimedata** angegeben haben, geben Sie an dieser Stelle ebenfalls diesen absoluten Pfad an. Beispiel:

  `c:\program files\crypt\smime\company.pfx`

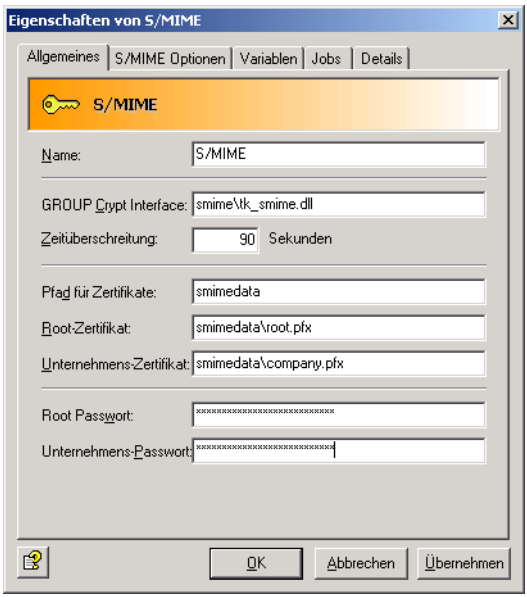
- **Root-Passwort:**

  Geben Sie hier das Passwort für das oben eingetragene Root-Zertifikat an. Das Passwort darf kein Leerzeichen enthalten.

- **Unternehmens-Passwort:**

  Geben Sie hier das Passwort für das oben eingetragene Unternehmens-Zertifikat an. Das Passwort darf kein Leerzeichen enthalten.

Fertig konfiguriert könnte diese Registerkarte so aussehen:



7.9.1.2 S/MIME Optionen einrichten

Wenn Sie die Zertifikate der Kommunikationspartner in einem LDAP Verzeichnis abgelegt haben, füllen Sie diese Felder bitte aus:

- **Parameter:**

  Bei der Verwendung eines LDAP Servers schreiben Sie in diese Zeile an das Ende *[LDAP]* dazu. Anschließend füllen Sie die Felder für den LDAP Zugriff aus.

- **LDAP Server:**

  Geben Sie den Servernamen oder die IP-Adresse des LDAP Servers ein. Beispiel: *server_home*

- **LDAP Port:**

  Geben Sie den LDAP Port ein. Als Standard LDAP Port ist *389* voreingestellt.

- **LDAP Pfad:**

  Bestimmen Sie hier den vollständigen LDAP Ast, in dem Sie suchen.

  Beispiel: `CN=Users,DC=Subdomain,DC=Domain,DC=DE`

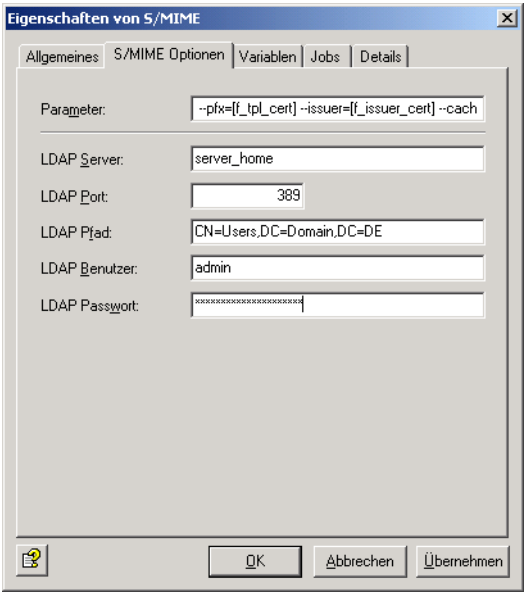
- **LDAP Benutzer:**

  Geben Sie den Benutzer(namen) an, der die Rechte für den LDAP Zugriff besitzt.

- **LDAP Passwort:**

  Hier geben Sie das für den oben eingetragenen Benutzer gültige Passwort ein. Das Passwort darf kein Leerzeichen enthalten.

Fertig konfiguriert könnte diese Registerkarte so aussehen:



7.9.1.3 Variablen

Die Variablen sind die für das GROUP Crypt Interface **tk_smime.dll** fertig konfiguriert und sollten nicht geändert werden.

7.9.1.4 Jobs überprüfen

Die Registerkarte **Jobs** zeigt, in welchen Jobs die S/MIME Crypt Engine verwendet wird.

7.9.1.5 Details

Die Eingabe der Job Details wird wie in der Beschreibung zu "Details zum Job eingeben" auf Seite 233 durchgeführt.

7.10 Verschlüsseln mit S/MIME

Auch bei der S/MIME-Verschlüsselung wird die Nachricht vom Absender mit dem öffentlichen Schlüssel - dem Zertifikat - des Empfängers verschlüsselt und nur der Empfänger kann die für ihn bestimmte Nachricht mit seinem privaten Schlüssel - Zertifikat - entschlüsseln.

S/MIME E-Mail-Nachrichten kann nur mit solchen Partnern ausgetauscht werden, deren E-Mail-Client auch den S/MIME-Standard implementiert hat. Hat Ihr Korrespondenzpartner ebenfalls iQ.Suite Crypt am Server installiert, so werden Verschlüsselung und Entschlüsselung direkt am Server durchgeführt und sind nicht mehr vom E-Mail-Client abhängig.

Die Konfiguration für iQ.Suite Crypt zur Verwendung von S/MIME erfolgt richtlinienbasiert, das bedeutet, die Adressen für Ver- und Entschlüsselung, Signatur und Signaturprüfung(-validierung) können dediziert für Nutzer, Nutzergruppen und das Unternehmen konfiguriert werden.

7.10.1 Ablauf der Verschlüsselung mit S/MIME

Vorgang: Eine Mail wird vom Client an einen Empfänger versendet, der die Mail verschlüsselt erhalten soll.

- Crypt schreibt die zu verschlüsselnden Daten in Form eines Multipart MIME Nachrichtentextes auf die Festplatte.
- Diese Datei und der/die Empfängername(n) wird/werden an das S/MIME-Interface übergeben. Dieses holt die Schlüssel vom LDAP Server (falls der Schlüssel noch nicht bekannt und ein LDAP Server konfiguriert ist) und verschlüsselt die Datei entsprechend.

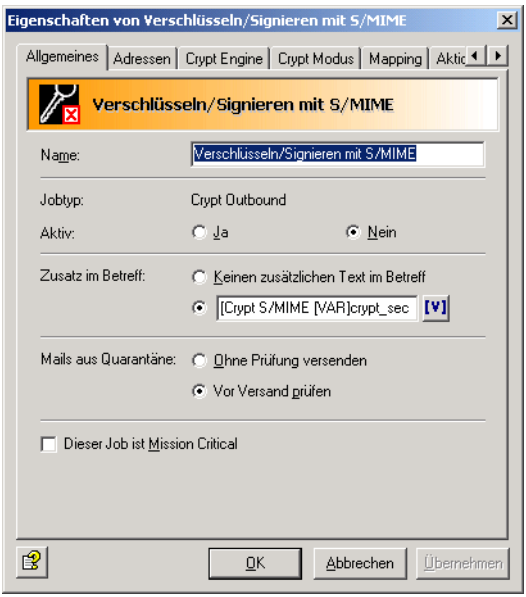
- Crypt fügt dann den so entstandenen S/MIME-Teil als neuen MIME Nachrichtentext in die Mail ein.

7.10.2 E-Mails mit S/MIME verschlüsseln - Jobbeispiel

Als Beispiel wird hier **Verschlüsseln/Signieren mit S/MIME** in der **Richtlinien-Konfiguration --> Jobbeispiele** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

7.10.2.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist mit einer Variablen (siehe “Liste der Benachrichtigungsvariablen” auf Seite 101) vordefiniert. Dieser Zusatz wird in den Betreff jeder Mail eingefügt, die erfolgreich verschlüsselt worden ist.

Dieser Job bearbeitet auch diejenigen Mails, die aus der **Quarantäne** wieder versendet werden. Die **Sende-Option** beim Versand aus der Quarantäne ist Jobübergreifend und hat Priorität. Wenn Sie eine Mail also mit der Quarantäne-Sende-Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die **Sende-Option** deshalb auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**.

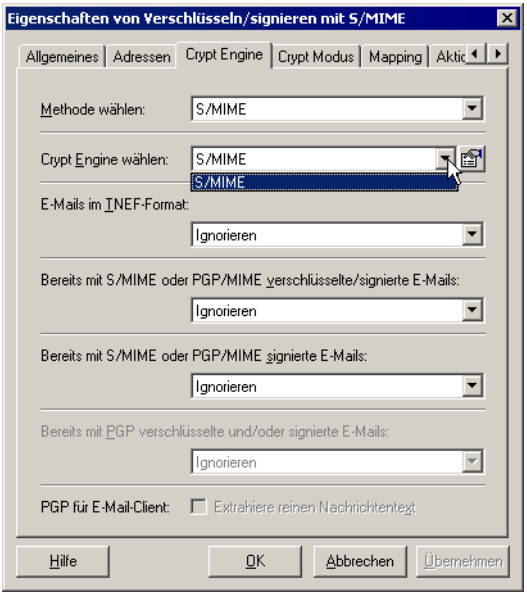
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

7.10.2.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

7.10.2.3 Crypt Engine auswählen - Verschlüsselungsmethode

In der Registerkarte **Crypt Engine** stellen Sie ein, welche Verschlüsselungsmethode und dazugehörige Optionen mit diesem Job aufgerufen werden sollen.



Die hier gewählte Verschlüsselungsmethode ist **S/MIME**. Die Crypt Engine ist automatisch **S/MIME**. Anschließend können Sie festlegen, wie Sie die Mail-Sonderfälle behandeln wollen. Dabei haben Sie folgende Möglichkeiten:

- **Ignorieren**

  Diese Mail wird nicht weiter von diesem Job behandelt, sondern an den nächsten Job weitergereicht.

- **Aktionen ausführen**

  Die definierten Aktionen auf der Registerkarte **Aktionen** werden ausgeführt.

- **Verarbeiten**

  Der Job behandelt die Mail genauso wie andere, die nicht unter diese Rubrik fallen.

Die einzelnen Sonderfälle:

- **E-Mails im TNEF-Format**

  Das Outlook-Format TNEF (**T**ransport **N**eutral **E**ncapsulation **F**ormat) kann nicht von iQ.Suite Crypt bearbeitet werden. Das TNEF-Format wird von

Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine E-Mail sendet. Bei der Kommunikation über das Internet bzw. bei der Verwendung von anderen E-Mail Programmen wird dieses Format nicht verwendet. Möchten Sie iQ.Suite Crypt auch für die interne Verschlüsselung nutzen, können Sie für TNEF-Mails die Optionen **Ignorieren** oder **Aktionen ausführen** wählen.

- **Bereits mit S/MIME oder PGP/MIME verschlüsselte/signierte E-Mails**
  E-Mails, die bereits verschlüsselt am Server ankommen, sind vom Client, also vom Benutzer verschlüsselt worden. Legen Sie in den E-Mail-Richtlinien Ihres Unternehmens fest, wie Sie solche Fälle behandeln wollen. Diese Einstellung gilt nur für Mails, die S/MIME oder PGP/MIME verschlüsselt oder verschlüsselt und signiert am Server eintreffen.

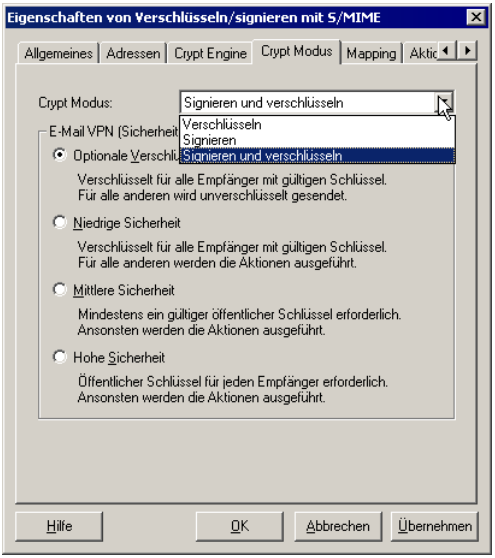
- **Bereits mit S/MIME oder PGP/MIME signierte E-Mails**
  Auch E-Mails, die bereits vom Benutzer signiert am Server ankommen, können Sie anders behandeln. Diese Einstellung gilt ebenfalls nur für Mails, die mit S/MIME oder PGP/MIME nur signiert und nicht verschlüsselt am Server ankommen.

- **Bereits mit PGP verschlüsselte oder signierte E-Mails**
  Diese Option ist bei einer Verschlüsselung mit S/MIME nicht verfügbar. Die Bedeutung dieser Einstellung entnehmen Sie bitte der Beschreibung in “Crypt Engine auswählen - Verschlüsselungsmethode” auf Seite 153.

- **Extrahiere reinen Nachrichtentext**
  Diese Option wird bei einer Verschlüsselung mit PGP/MIME und S/MIME nicht benötigt und ist daher nicht verfügbar. Die Bedeutung dieser Einstellung entnehmen Sie bitte ebenfalls der Beschreibung in “Crypt Engine auswählen - Verschlüsselungsmethode” auf Seite 153.

7.10.2.4 Crypt Modus auswählen - Verschlüsselungsmodus - VPN

In der Registerkarte **Crypt Modus** stellen Sie ein, welcher Verschlüsselungsmodus und welche **Sicherheitseinstellungen** (VPN Kanal) mit diesem Job aufgerufen werden sollen.



Der hier gewählte **Crypt Modus** ist **Signieren und verschlüsseln**. Die Möglichkeiten sind:

- **Signieren und verschlüsseln**

  Die Mail wird gleichzeitig signiert und verschlüsselt.

- **Verschlüsseln**

  Die Mail wird nur verschlüsselt und nicht signiert.

- **Signieren**

  Die Mail wird nur signiert und nicht verschlüsselt.

Die einzelnen Optionsmöglichkeiten zeigen die möglichen **Sicherheitseinstellungen** für ausgehende E-Mails (**VPN** Kanäle). Alle Optionen gelten nur für die Verschlüsselung, da das Signieren mit dem privaten Zertifikat erfolgt, bei Fehlen dieses Zertifikats sofort fehlschlägt und die definierten **Aktionen** durchgeführt werden.

- **Optionale Verschlüsselung**

  Die Mails werden mit den vorhandenen öffentlichen Zertifikaten verschlüsselt. Allen Empfängern, für die kein gültiges Zertifikat vorliegt, erhalten die Mail unverschlüsselt.

Niedrige Sicherheit

Die Mails werden mit den vorhandenen öffentlichen Zertifikaten verschlüsselt. Die Adressaten mit gültigem Zertifikat erhalten die Mail verschlüsselt. Für alle Empfänger ohne gültiges Zertifikat werden die auf der Registerkarte **Aktionen** definierten Maßnahmen durchgeführt.

Mittlere Sicherheit

Die Mails werden nur dann mit den vorhandenen öffentlichen Zertifikaten verschlüsselt, wenn **mindestens ein gültiges Zertifikat** vorliegt. Alle Adressaten erhalten die Mail verschlüsselt. Die Adressaten mit gültigem Zertifikat können die Mail mit ihrem privaten Zertifikat öffnen. Alle Empfänger ohne gültiges Zertifikat werden also die verschlüsselte Mail nicht öffnen können, da sie kein passendes privates Zertifikat zu den verwendeten öffentlichen Zertifikaten besitzen. Die auf der Registerkarte **Aktionen** definierten Maßnahmen werden nur durchgeführt, wenn überhaupt kein gültiges Zertifikat vorhanden ist.

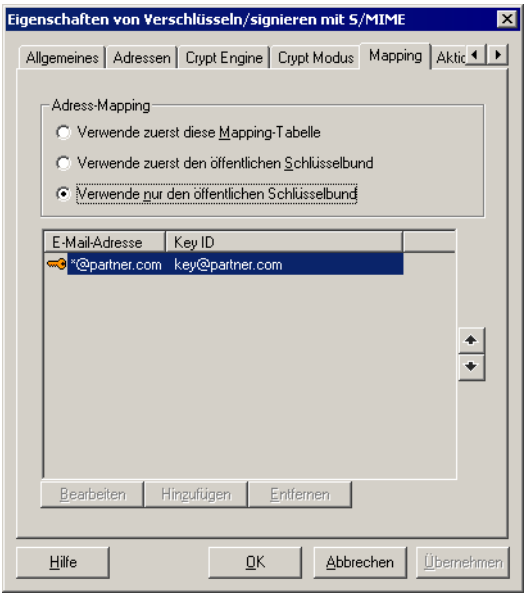
Hohe Sicherheit

Die Mails werden nur dann mit den vorhandenen öffentlichen Zertifikaten verschlüsselt, wenn **für alle Adressaten ein gültiges Zertifikat** vorliegt. Die auf der Registerkarte **Aktionen** definierten Maßnahmen treten sofort in Kraft, wenn nur ein einziges Zertifikat ungültig ist oder fehlt.

Ein Job kommt nur für diejenigen Adressaten zur Ausführung, die Sie in der Registerkarte **Adressen** festgelegt haben. Wenn Sie dort nur die Kommunikationspartner mit einem gültigen öffentlichen Zertifikat eintragen, können Sie mit der Auswahl einer hohen Sicherheitseinstellung „abhörsichere“ Kanäle schaffen, ohne dass Fehler wegen fehlender Zertifikate auftreten und die definierten **Aktionen** durchgeführt werden. Legen Sie für jede Sicherheitseinstellung einen Job an, also zwei Jobs, wenn Sie Mails für einige Adressen sehr sicher übertragen wollen und alle anderen Kommunikationspartner nur optional verschlüsselt werden sollen.

7.10.2.5 Mapping auswählen - Key ID-Zuordnung

In der Registerkarte **Mapping** bestimmen Sie die Art des Adressmappings für die Verschlüsselung und erstellen bei Bedarf Ihre eigene Mapping-Tabelle.



Die Voreinstellung ist **Verwende nur den öffentlichen Schlüsselbund**. Die Möglichkeiten sind:

- **Verwende zuerst diese Mapping-Tabelle**

  Die Einträge in der unten stehenden selbst definierten Mapping-Tabelle haben Vorrang. Wenn in dieser Tabelle zu einer Empfängeradresse eine Key ID eingetragen ist, wird in der Cache DB nach dieser Key ID gesucht und das dazu gehörige Zertifikat verwendet. Erst wenn kein passender Eintrag in der Tabelle gefunden worden ist, sucht der Verschlüsselungsjob in der Cache DB unter der Empfänger-Adresse als Key ID. Die Key ID muss hier die E-Mail-Adresse sein, die im Zertifikat hinterlegt ist. Diese Einstellung ist sinnvoll, wenn über sichere VPN Kanäle eine Verschlüsselung mit einem bestimmten Unternehmen verwirklicht werden soll.

- **Verwende zuerst den öffentlichen Schlüsselbund**

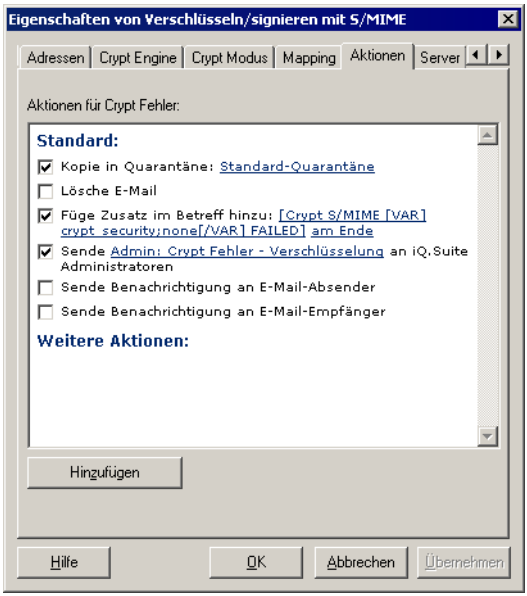
  Die Einträge in der Cache DB haben Vorrang. Erst wenn kein zur Empfängeradresse passender Eintrag in der Cache DB gefunden worden ist, sucht der Job in der unten stehenden Mapping-Tabelle nach einer Key ID.

- **Verwende nur den öffentlichen Schlüsselbund**

  Die Zertifikate werden ausschließlich anhand der Empfängeradresse in der Cache-DB gesucht. In diesem Fall wird die Mapping-Tabelle nicht aktiviert; evtl. Einträge bleiben aber erhalten.

7.10.2.6 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn die Verschlüsselung durch den Job fehlgeschlagen ist.



Als Aktion wird eine Kopie in die Quarantäne gestellt. Das beinhaltet, dass die Mail dem Empfänger trotzdem zugestellt wird. Eine Benachrichtigung über die nicht erfolgte Verschlüsselung wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt. Diese können individuell über die HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[20].

7.10.2.7 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu "Server auswählen" auf Seite 233 und "Details zum Job eingeben" auf Seite 233 durchgeführt.

7.11 Entschlüsseln mit S/MIME

7.11.1 Ablauf der Entschlüsselung mit S/MIME

Vorgang: Eine verschlüsselte Mail soll beim Eintreffen auf dem Server entschlüsselt werden.

- Crypt schreibt die zu entschlüsselnden Daten in Form eines Multipart MIME Nachrichtentextes auf die Festplatte.
- Diese Datei wird an das S/MIME-Interface übergeben. Anschließend wird die Mail mit dem privaten Schlüssel entschlüsselt.
- Crypt fügt dann den so entstandenen MIME Teil als neuen MIME Nachrichtentext in die Mail ein.

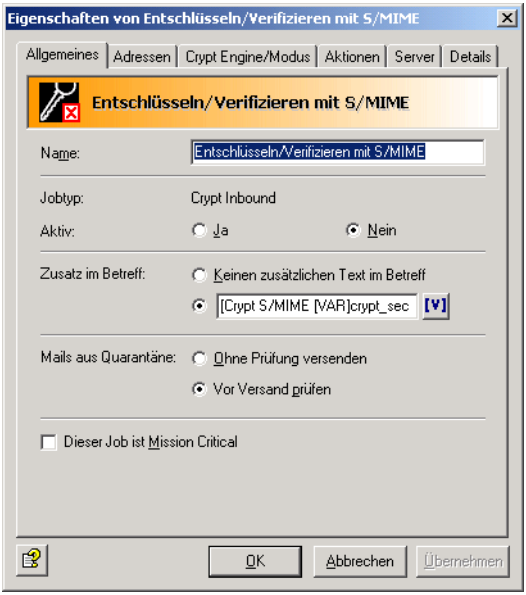
7.11.2 E-Mails mit S/MIME entschlüsseln - Jobbeispiel

Als Beispiel wird hier **Entschlüsseln/Verifizieren mit S/MIME** in der **Richtlinien-Konfiguration --> Jobbeispiele** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

7.11.2.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.

20. siehe dazu "Benachrichtigungsvorlagen erstellen" auf Seite 100



Der **Zusatz im Betreff** ist mit einer Variablen (siehe “Liste der Benachrichtigungsvariablen” auf Seite 101) vordefiniert. Dieser Zusatz wird in den Betreff jeder Mail eingefügt, die erfolgreich entschlüsselt worden ist.

Dieser Job bearbeitet auch diejenigen Mails, die aus der **Quarantäne** wieder versendet werden. Die **Sende-Option** beim Versand aus der Quarantäne ist Jobübergreifend und hat Priorität. Wenn Sie eine Mail also mit der Quarantäne-Sende-Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die **Sende-Option** deshalb auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

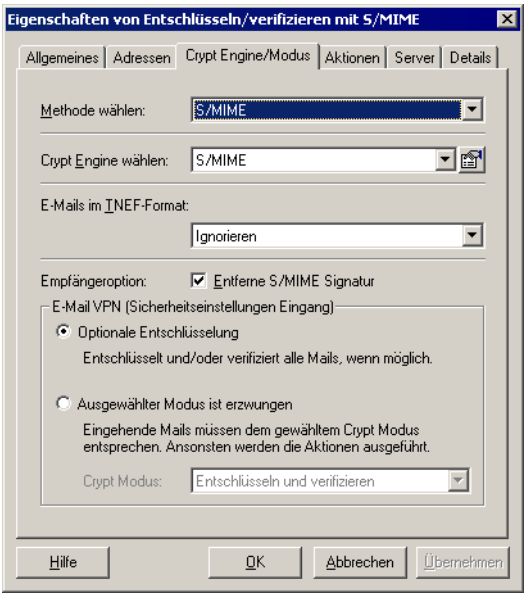
7.11.2.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhan-

denen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

7.11.2.3 Crypt Engine/Modus auswählen - Methode

In der Registerkarte **Crypt Engine/Modus** stellen Sie ein, welche Entschlüsselungsmethode und welche Sicherheitseinstellungen mit diesem Job aufgerufen werden sollen. Außerdem können Sie hier Zusatzoptionen einrichten.



Die hier gewählte Entschlüsselungsmethode ist **S/MIME**. Die Crypt Engine ist **TK_S/MIME**. Anschließend können Sie die Optionen festlegen.

Die einzelnen Optionen:

- **E-Mails im TNEF-Format**

  Das Outlook-Format TNEF (**T**ransport **N**eutral **E**ncapsulation **F**ormat) kann nicht von iQ.Suite Crypt bearbeitet werden. Das TNEF-Format wird von Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine E-Mail sendet. Bei der Kommunikation über das Internet bzw. bei der Verwendung von anderen E-Mail

Programmen wird dieses Format nicht verwendet. Möchten Sie iQ.Suite Crypt auch für die interne Verschlüsselung nutzen, können Sie für TNEF-Mails die Optionen **Ignorieren** oder **Aktionen ausführen** wählen.

- **Ignorieren**
  Diese Mail wird nicht weiter von diesem Job behandelt, sondern an den nächsten Job weitergereicht.
- **Aktionen ausführen**
  Die definierten Aktionen auf der Registerkarte **Aktionen** werden ausgeführt.

- **Für Empfänger: Entferne S/MIME Signatur**
  E-Mails, die mit S/MIME signiert worden sind, können mit Crypt bereits am Server auf gültige Signatur geprüft werden. iQ.Suite Crypt kann die Signatur ablösen, so dass der Endbenutzer, also der Empfänger der Mail, von der Signaturprüfung nichts bemerkt (=Voreinstellung). Diese Einstellung ist nur dann verfügbar, wenn die Entschlüsselungsmethode PGP/MIME oder S/MIME ist.

Modus und Sicherheitseinstellungen (VPN Kanäle):

Die einzelnen Optionsmöglichkeiten zeigen die möglichen **Sicherheitseinstellungen** für eingehende E-Mails (**VPN** Kanäle). Die Voreinstellung ist **Optionale Entschlüsselung**.

Es gibt für die Entschlüsselung zwei mögliche Sicherheitseinstellungen:

- **Optionale Entschlüsselung**
  Die Mails werden - wenn möglich - mit den vorhandenen privaten Zertifikaten entschlüsselt und die Signatur - wenn möglich - mit den vorhandenen öffentlichen Zertifikaten verifiziert. Sollte eine Mail nicht verschlüsselt oder signiert sein, erhalten die Empfänger die Mails so wie sie sind. Tritt bei der Entschlüsselung oder Verifizierung ein Fehler auf, z.B. weil das private Zertifikat fehlt oder die Mail verändert wurde und damit nicht verifiziert werden kann, so werden die konfigurierten Aktionen ausgeführt.

Ausgewählter Modus ist erzwungen

Es werden nur diejenigen eingehenden E-Mails an den Empfänger weitergegeben, die exakt dem ausgewählten Modus im Pull-Down-Menü entsprechen. Wenn Sie also beispielsweise **Verifizieren und entschlüsseln** wählen, dann müssen die eingehenden Mails sowohl signiert als auch verschlüsselt sein. Die Bedingung gilt als nicht erfüllt, wenn die Mail nur verschlüsselt eingeht und nicht signiert ist. Für alle Mails, die dem ausgewählten Modus nicht entsprechen, werden die auf der Registerkarte **Aktionen** definierten Maßnahmen durchgeführt. Sie können folgende Modi auswählen:

- **Entschlüsseln und verifizieren**

  Die Mail wird gleichzeitig entschlüsselt und verifiziert. Unter diese Bedingung fallen nur diejenigen Mails, die signiert **und** verschlüsselt am Server ankommen.

- **Entschlüsseln**

  Die Mail wird nur entschlüsselt. Nur signierte oder signierte und verschlüsselte Mails fallen nicht unter diese Bedingung.

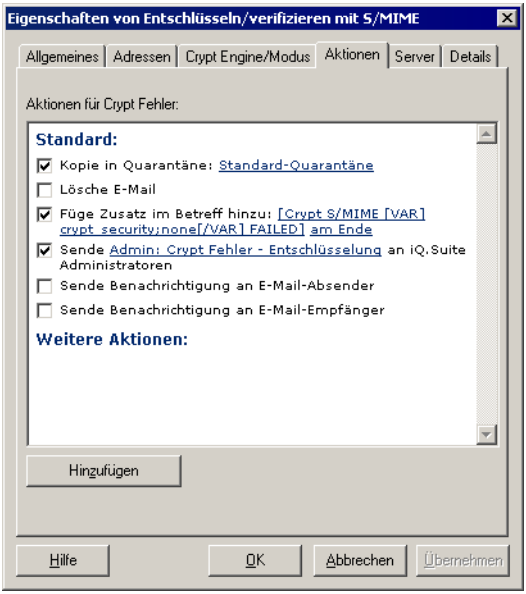
- **Verifizieren**

  Die Mail wird nur verifiziert. Nur verschlüsselte oder signierte und verschlüsselte Mails fallen nicht unter diese Bedingung.

Ein Job kommt nur für diejenigen Adressaten zur Ausführung, die Sie in der Registerkarte **Adressen** festgelegt haben. Wenn Sie dort nur die Kommunikationspartner eintragen, mit denen Sie beispielsweise vereinbart haben, dass alle E-Mails sowohl signiert als auch verschlüsselt übertragen werden sollen, können Sie mit der Auswahl des erzwungenen Modus „abhörsichere“ Kanäle schaffen, ohne dass Fehler wegen einer Mail im falschen Modus auftreten und die definierten **Aktionen** durchgeführt werden. Legen Sie für jede Sicherheitseinstellung einen Job an, also zwei Jobs, wenn Sie Mails für einige Adressen sehr sicher übertragen wollen und alle anderen Kommunikationspartner nur optional entschlüsselt bzw. verifiziert werden sollen.

7.11.2.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn die Entschlüsselung bzw. Verifizierung durch den Job fehlgeschlagen ist.



Als Aktion wird eine Kopie in die Quarantäne gestellt. Das beinhaltet, dass die Mail dem Empfänger trotzdem zugestellt wird. Eine Benachrichtigung über die nicht erfolgte Entschlüsselung wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt. Diese können individuell über die HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[21].

7.11.2.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

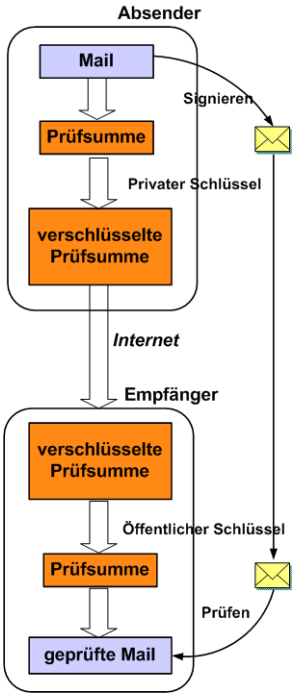
21. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100

7.12 Signieren mit S/MIME

iQ.Suite Crypt unterstützt außerdem die digitale Signatur mit S/MIME. Eine digitale Signatur identifiziert den Absender wie eine Unterschrift und ermöglicht dem Empfänger festzustellen, dass die Nachricht tatsächlich vom angegebenen Absender gesendet wurde und auf dem Übertragungsweg nicht verändert wurde. Die Signatur verhindert nicht, dass die Nachricht auf dem Übertragungsweg eingesehen werden kann. iQ.Suite Crypt kann auf solche Weise signierte E-Mails im Ganzen wiederum verschlüsseln. Die Signatur wird mit dem privaten Schlüssel erstellt und mit dem öffentlichem Schlüssel beim Empfänger auf Echtheit geprüft.

Grafisch etwas vereinfacht sieht das etwa so aus:

S/MIME-Signatur



7.12.1 Ablauf für S/MIME Signaturen

Vorgang: Eine Mail wird vom Client an einen Empfänger versendet, der die Mail signiert erhalten soll.

- Crypt schreibt die zu signierenden Daten auf die Festplatte.
- Diese Datei wird an das S/MIME-Interface übergeben. Dieses holt das Unternehmens-Zertifikat, erstellt für den Absender eine Kopie des Schlüssels und fügt dessen E-Mail-Adresse ein.
- Dieses erstellte Zertifikat wird mit dem Root-Zertifikat signiert, damit es gültig wird.
- Die zu signierenden Daten werden mit dem erstellten Schlüssel signiert.
- Crypt fügt dann den so entstandenen S/MIME-Teil als neuen MIME Nachrichtentext in die Mail ein und hängt das öffentliche Zertifikat an.

Bei einigen Clients muss die E-Mail-Adresse des Zertifikats mit dem die Mail signiert wurde, mit der Adresse des Absenders übereinstimmen. Deshalb wird vom S/MIME-Interface ein neuer Schlüssel erstellt, der die E-Mail-Adresse des Absenders enthält.

7.12.2 E-Mails mit S/MIME signieren - Job einrichten

Wenn Sie E-Mails mit S/MIME nur signieren möchten, so verwenden Sie den Job **Entschlüsseln/Verifizieren mit S/MIME**, ziehen diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und ändern ihn folgendermaßen:

1. Benennen Sie den Job nach seiner Funktion um.
2. Setzen Sie auf der Registerkarte **Crypt Modus** die Verschlüsselungsmethode auf **Signieren**.
3. Legen Sie unter Crypt Engine die Behandlung des Sonderfalls **Bereits mit S/MIME oder PGP/MIME signierte E-Mails** fest.

Eine genaue Beschreibung der einzelnen Felder finden Sie im Kapitel “E-Mails mit S/MIME verschlüsseln - Jobbeispiel” auf Seite 173.

7.13 Verifizieren (prüfen) von S/MIME Signaturen

Beim Eingang auf dem Server wird die mit S/MIME signierte Mail mit dem öffentlichen Zertifikat des Absenders auf Gültigkeit geprüft (verifiziert) und damit der angegebene Absender identifiziert.

7.13.1 Ablauf der S/MIME Verifikation

Vorgang: Eine signierte MIME-Mail geht auf dem Server ein. Die Signatur soll geprüft werden.

- Crypt schreibt die zu signierten Daten und die Signatur auf die Festplatte.
- Diese Datei wird an das S/MIME-Interface übergeben. Dieses holt das öffentliche Zertifikat des Absenders aus der Mail oder der Cache DB (bei fehlendem Zertifikat optional vom LDAP-Server) und prüft die Signatur.
- Crypt fügt dann den so entstandenen MIME Teil (ohne Signatur!) als neuen MIME Nachrichtentext in die Mail ein.

Die S/MIME Crypt Engine importiert die Zertifikate automatisch in die Cache DB. Daher ist ein Importieren der Zertifikate (oder ein Import-Job) nicht notwendig.

7.13.2 E-Mail-Signaturen mit S/MIME prüfen - Job einrichten

Wenn Sie im Job **Entschlüsseln/Verifizieren mit S/MIME** die Sicherheitseinstellungen auf **Optionale Entschlüsselung** eingestellt haben, so werden alle Signaturen - so sie vorhanden sind - automatisch geprüft, genauso wie verschlüsselte Mails automatisch entschlüsselt werden.

Wenn Sie zwingend nur signierte E-Mails erlauben möchten, so verwenden Sie den Job **Entschlüsseln/Verifizieren mit S/MIME**, ziehen diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und ändern ihn folgendermaßen:

1. Benennen Sie den Job nach seiner Funktion um.
2. Setzen Sie auf der Registerkarte **Crypt Engine/Modus** die Sicherheitseinstellung auf **Ausgewählter Modus ist erzwungen** und die Entschlüsselungsmethode auf **Verifizieren**.

Eine genaue Beschreibung der einzelnen Felder finden Sie im Kapitel “E-Mails mit S/MIME entschlüsseln - Jobbeispiel” auf Seite 181.

8 iQ.Suite Trust

In einer Public Key-Infrastruktur (PKI) werden die öffentlichen Schlüssel (öffentlicher Schlüssel, siehe auch privater Schlüssel) in einer Datenbank verwaltet. Um die Authentizität der Schlüsselpaare zu gewährleisten, müssen diese beglaubigt (zertifiziert) werden. Die Zertifizierung kann durch ein externes Trustcenter (CA), z.B. bei VeriSign, vorgenommen werden. Das kann je nach Anzahl der zertifizierten Schlüsselpaare und der Häufigkeit der Zertifizierung sehr kostenintensiv werden.

iQ.Suite Trust ist vergleichbar mit einem Trustcenter. Mit iQ.Suite Trust können durch eine CA zertifizierte Schlüsselpaare (Zertifikate) erstellt werden.

Die Registrierung und Zertifizierung ist dabei nicht von einer externen Stelle abhängig, sondern kann nach unternehmensinternen Richtlinien vorgenommen werden, was sich in der Regel einfacher administrieren lässt und insgesamt kostengünstiger ist.

iQ.Suite Trust ist ein Offline-Administrationswerkzeug. Das heißt, dass die bearbeitete CA lokal gesichert ist und erst nach der Bearbeitung ein Einspielen in den produktiven LDAP-Verzeichnisdienst erfolgt.

Eine detaillierte Bedienungsanleitung finden Sie im separaten iQ.Suite Trust Handbuch, welches Sie sich auf der Dokumentations-Website herunterladen können.

9 iQ.Suite Trailer

9.1 Übersicht

iQ.Suite Trailer ist das Modul für die Integration von Textbausteinen in die Fußzeile einer E-Mail. Mit Textbausteinen können Sie jeden Text wie Firmeninformationen, Rechtshinweise oder individuelle Signaturen integrieren. Ein einheitliches Erscheinungsbild Ihres Unternehmens und die Corporate Identity können so leicht nach außen transportiert werden. Trailer kann einen oder mehrere Texte in ASCII oder HTML-Format anhängen.

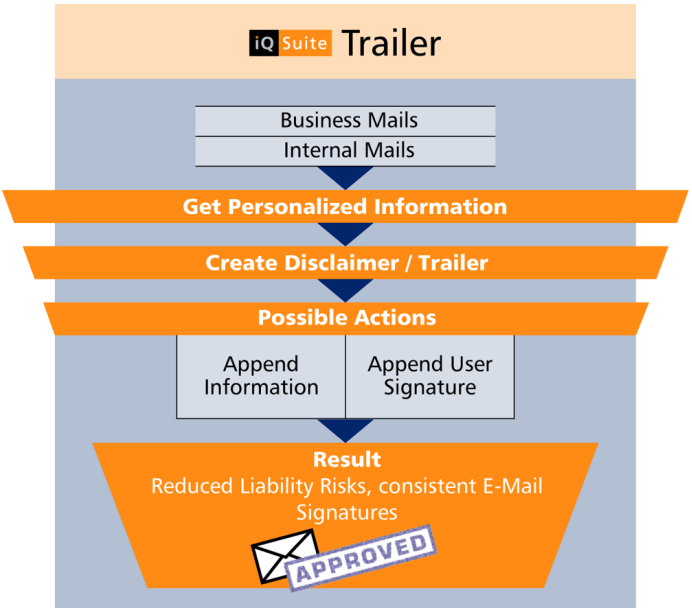
9.1.1 Jobtyp

- zentrales Anhängen von Textbausteinen oder Signaturen

  Job: **Trailer**

Die genaue Vorgehensweise entnehmen Sie bitte den Beschreibungen ab “Erstellen eines neuen Textbaustein-Trailers” auf Seite 194.

Grafisch dargestellt sieht die Arbeitsweise wie folgt aus:



9.2 Anhängen von Textbausteinen

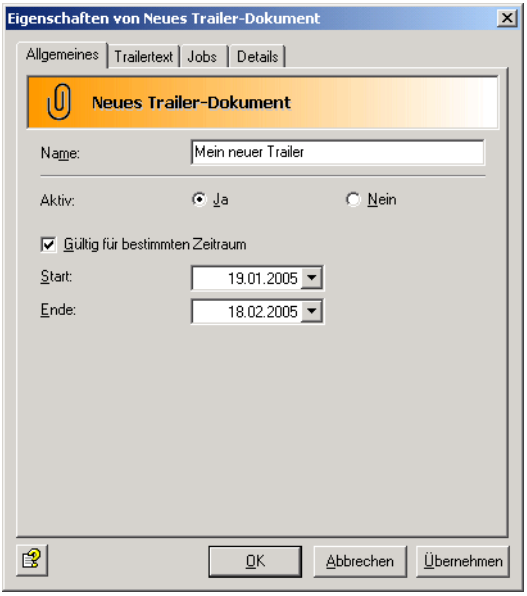
Die einzelnen Textbausteine werden als Trailerdokument angelegt, mit einem sprechenden Namen versehen und in der iQ.Suite Konfiguration abgelegt. Im Trailer-**Job** wird der gewünschte Text aus einer Liste ausgewählt. Der Ablauf in einzelnen Schritten:

1. Erstellen Sie ein neues Trailerdokument.
2. Bestimmen Sie einen Gültigkeitszeitraum und aktivieren Sie das Dokument.
3. Erstellen Sie einen Trailer-Job und wählen Sie den neuen Trailer aus.
4. Aktivieren Sie den Job.

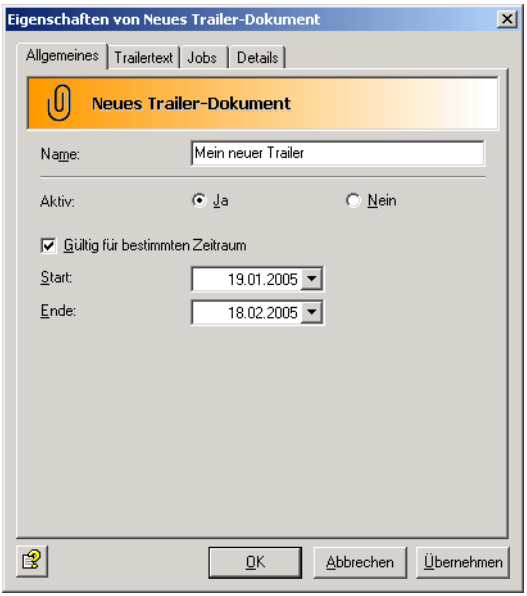
9.2.1 Erstellen eines neuen Textbaustein-Trailers

Um einen Trailer zentral anhängen zu können, muss das Trailer-Dokument existieren, also vor dem Job erstellt werden.

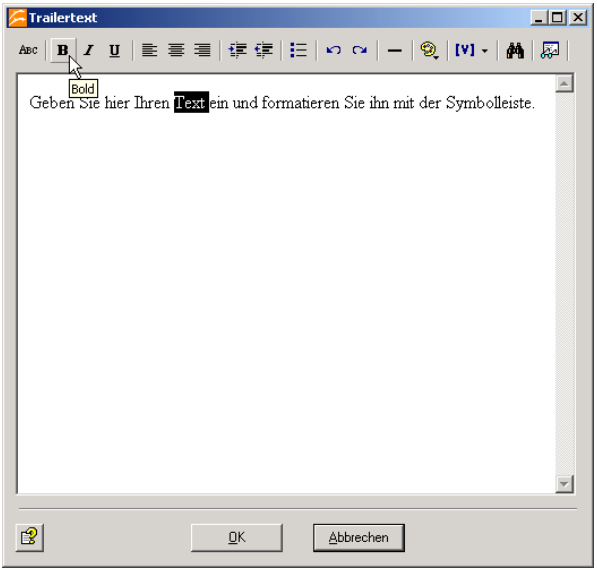
1. Klicken Sie auf den **Trailer**-Ordner unter **Basis Konfiguration --> Allgemeine Einstellungen**.
2. Drücken Sie die rechte Maustaste und klicken Sie auf **Neu --> Trailer**. Sie erhalten den Dialog für ein neues Trailerdokument.
3. Bestimmen Sie den Zeitraum für diesen Trailer. Wenn Sie keinen Zeitraum setzen, ist dieser Trailer unbegrenzt gültig. Setzen Sie ihn **Aktiv**.



4. Klicken Sie auf **Trailertext** und dort auf **Bearbeiten**. Sie erhalten das Eingabefenster:



5. Schreiben Sie Ihren Text. Formatieren Sie ihn mit Hilfe der Symbolleiste. Diese Formatierungen werden intern in HTML umgesetzt. Andere HTML-Befehle sind nicht möglich! Klicken Sie anschließend **OK**.



6. In welchen Jobs der Trailer verwendet wird, ersehen Sie aus der Registerkarte **Jobs**.
7. Speichern Sie den Trailer mit **OK**.

Der Text für einen Trailer sollte zusammen mit den Fachabteilungen entworfen werden.

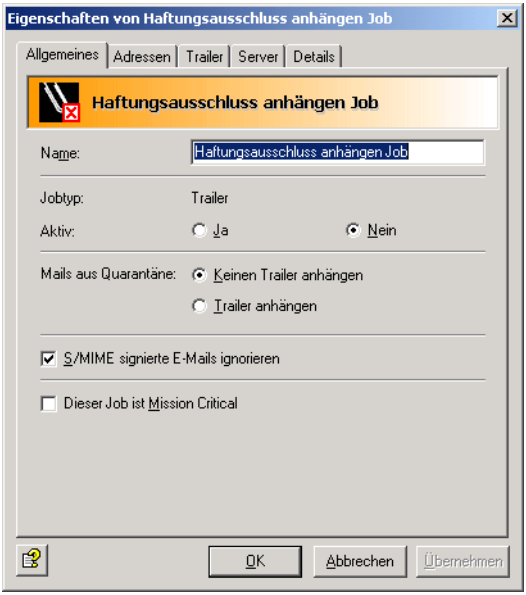
Kopieren Sie unseren vorkonfigurierten Trailer **Legal Disclaimer**, den Sie in der Standard-Konfiguration vorfinden und passen Sie diesen für Ihre Zwecke an.

9.2.2 Haftungsausschluss anhängen - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Mail Transport Jobs** finden Sie den Job **Haftungsausschluss anhängen.** Öffnen Sie diesen mit einem Doppelklick.

9.2.2.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

Das heißt, in diesem Fall wird kein Trailer angehängt. Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

Dieser Job ignoriert Mails, die vom Client aus signiert (S/MIME-Signatur) versendet werden, da iQ.Suite Trailer die Mail öffnen muss, um den Textbaustein zu integrieren. Dadurch würde eine Signatur ungültig.

9.2.2.2 Adressbedingungen einrichten

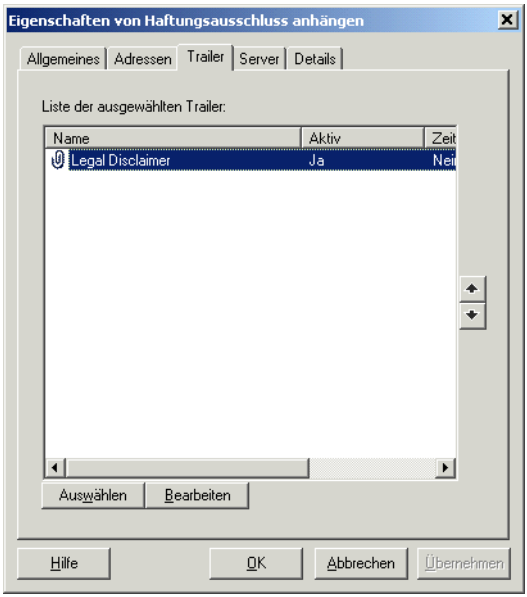
Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

Bedenken Sie bitte bei der Einrichtung der Adressbedingungen, dass Mailinglisten und ähnliche Adressen keinen Trailer erhalten sollten! Richten Sie solche Ausnahmen in den Adressbedingungen unter der Option **gilt aber nicht für diese „Empfänger“** ein.

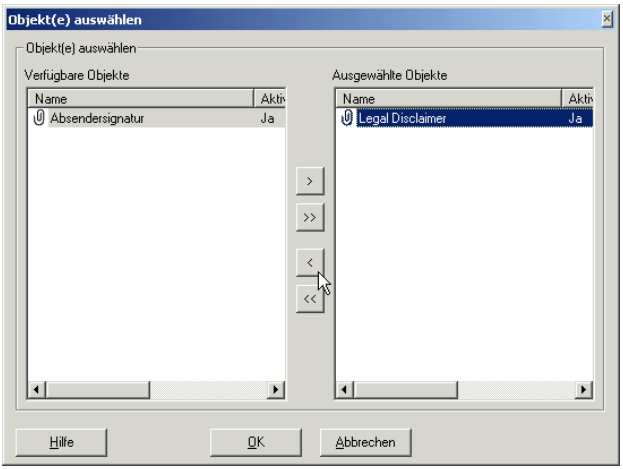
Sie können einen Trailer ausschließlich für eine bestimmte Abteilung einrichten, wenn Sie eine Gruppenliste auswählen.

9.2.2.3 Trailer auswählen

Wählen Sie unter der Registerkarte **Trailer** den gewünschten Trailer aus.

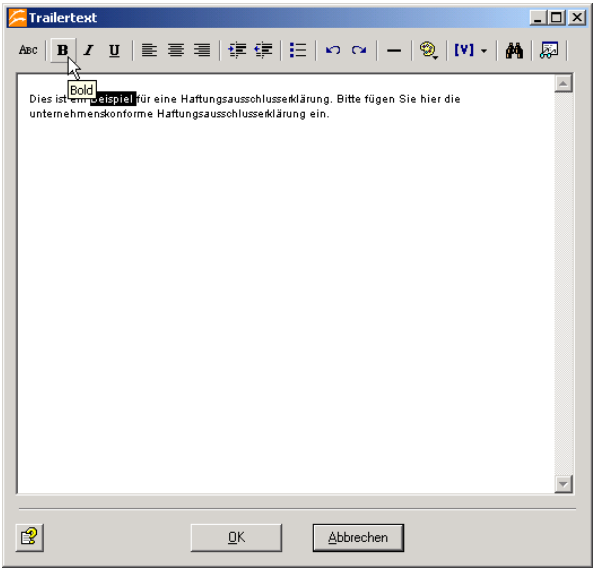


Mit der Schaltfläche **Auswählen** können Sie einen anderen Trailer anhängen, sofern dieser vorher angelegt worden ist oder einen bestehenden aus dem Job entfernen. Benutzen Sie dazu die Pfeiltasten [>] und [<] im Auswahlmenü:



Die Standardkonfiguration enthält bereits einen **Legal Disclaimer**. Passen Sie diesen an Ihre eigenen Unternehmensrichtlinien an. Dazu klicken Sie auf **Bearbeiten** und anschließend auf die Registerkarte **Trailertext**:

Klicken Sie auf **Bearbeiten**:



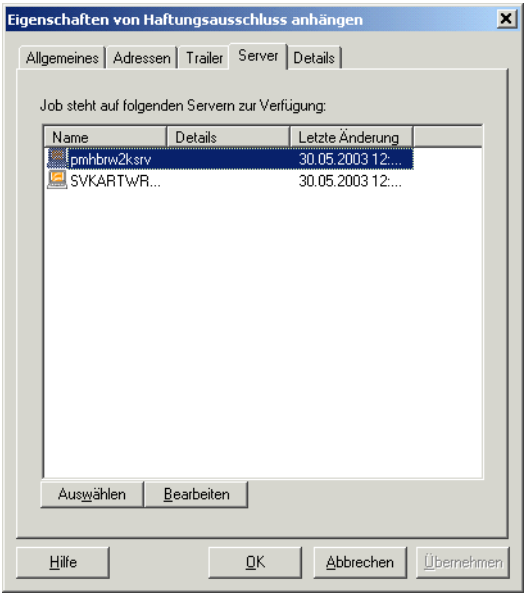
Passen Sie den Text an Ihre eigenen Unternehmensrichtlinien an und klicken Sie **OK**[22].

Sprechen Sie mit den Fachabteilungen über die Unternehmensrichtlinien und den Inhalt der Trailer-Texte.

9.2.2.4 Server auswählen

Auf der Registerkarte **Server** wählen Sie den oder die Server aus, auf denen der Job aktiv sein soll.

22. Zur Bearbeitung von Trailertexten siehe
"Erstellen eines neuen Textbaustein-Trailers" auf Seite 194



Klicken Sie auf die Schaltfläche **Auswählen**. Sie erhalten einen zu der Auswahl von Virenscannern analogen Dialog, siehe auch "Virenscanner auswählen" auf Seite 226.

.

Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein. Näheres zur Konfiguration von iQ.Suite Servern finden Sie in "Einstellungen für einen einzelnen iQ.Suite Server" auf Seite 85ff.

Da Sie einen Trailer nur an ausgehende Mails anhängen wollen, wählen Sie hier nur den Mailausgangsserver!

9.2.2.5 Details zum Job eingeben

Auf der letzten Registerkarte **Details** können Sie den Job näher beschreiben:

9.3 Anhängen von individuellen Signaturen

iQ.Suite Trailer kann absenderabhängige Informationen direkt am Server in die E-Mails einfügen. Dadurch können Sie in Kombination mit Bedingungen automatisch unterschiedliche „Signaturen“ für verschiedene Personen oder Abteilungen kreieren, ohne die Informationen redundant halten zu müssen. Unter Signatur verstehen wir an dieser Stelle keine digitale Unterschrift, sondern Grußformeln und die Absenderangaben.

Einheitliche Signaturen gewährleisten eine konsequent einheitliche Außendarstellung des Unternehmens. Dadurch wird verhindert, dass die eine Abteilung Goethezitate verwendet und die andere Monty Python, dass die eine Signatur Gebäude und Raumnummer des Mitarbeiters enthält, die andere nur Telefon und Faxnummer. Jeder Geschäftsbrief gewährleistet eine gewisse Einheitlichkeit im Layout und das sollte auch für die Kommunikation per E-Mail gelten. Unabhängig davon, ob die E-Mail-Benutzersignatur statische Texte beinhaltet, sollte sie die wichtigsten Angaben zum Absender liefern, und das sind nun einmal die so genannten "Koordinaten". Der einfachste Weg ist es, Signaturen zentral zu erstellen und zuzuweisen. Werden die Vorgänge serverbasiert durchgeführt, sind Aktualität, Richtigkeit und vor allen Dingen unternehmensweite Einheitlichkeit der Informationen gewährleistet, auch bei Umzug, Wechsel der Telefon- und Raumnummern und neuen Abteilungsstrukturen.

iQ.Suite Trailer entnimmt die nötigen Informationen dem Active Directory. Dessen Domänenstruktur lässt sich einfach pflegen und leicht um Objekte und Eigenschaften erweitern. Um den Zugriff auf domänenübergreifende Informationen zu ermöglichen, verwendet iQ.Suite Trailer den Global Catalog. Dieser entspricht einem Index, der die relevanten Informationen aller Benutzer eines Active Directorys beinhaltet. Es werden dabei keinerlei Veränderungen am Active Directory vorgenommen. Vielmehr handelt es sich um einen rein lesenden Zugriff.

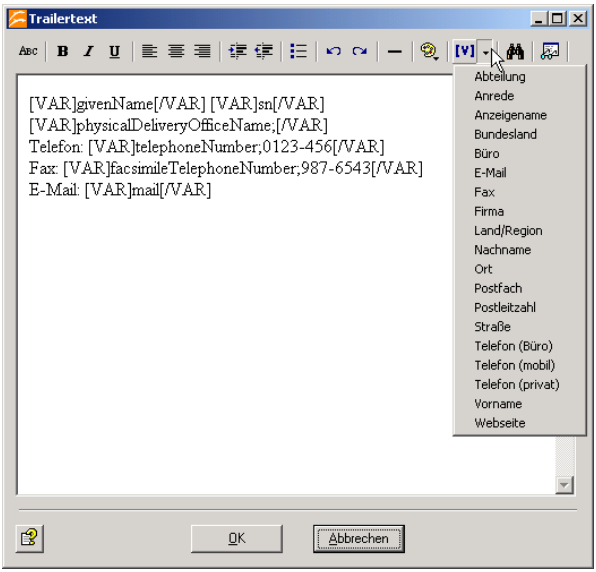
Bei der Erstellung eines neuen Trailers können die möglichen Variablen für Vor- und Nachname, Abteilung usw. aus einer Drop Down Liste ausgewählt werden. Ist ein Wert nicht vorhanden, lässt sich ein allgemeingültiger Standardwert einfügen.

Es kann auch jeder andere Wert aus dem Active Directory "angezapft" werden. Verwendet ein Unternehmen beispielsweise benutzerdefinierte Attribute im AD, um die Personalnummern zu hinterlegen, kann auch diese Informationen von Trailer genutzt werden. Lesen Sie zu diesem Zweck die Active Directory-Werte mit ADSI Edit[23] aus.

9.3.1 Erstellen eines neuen Trailers für individuelle Signaturen

Gehen Sie zunächst analog zu "Erstellen eines neuen Textbaustein-Trailers" auf Seite 194 vor.

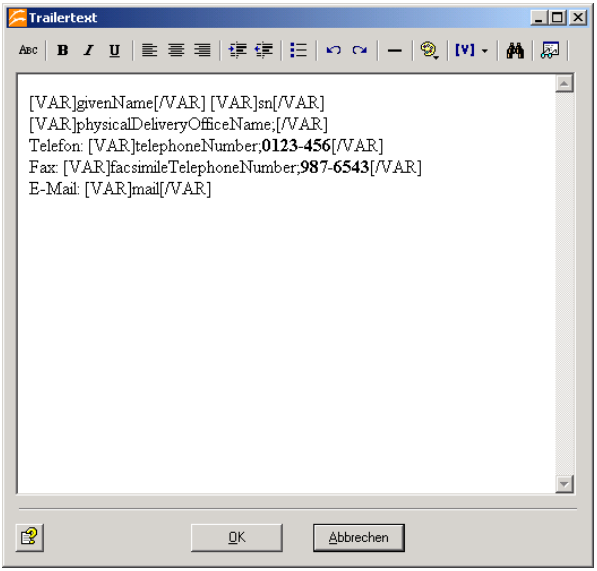
1. Individuelle Signaturen werden in der Regel ohne Gültigkeitszeitraum angelegt. Achten Sie darauf, dass in der Registerkarte **Allgemeines** die Checkbox **Gültig für bestimmten Zeitraum** deaktiviert ist.
2. Klicken Sie in der Registerkarte **Trailertext** auf **Bearbeiten**.
3. Klicken Sie im Bearbeitungsfenster auf das Symbol für die Variablen:



4. Wählen Sie die gewünschten Informationen aus.
5. Die Variablen erscheinen im Eingabefenster und können nach den Richtlinien des Unternehmens formatiert werden: Leerzeichen, Striche, Fettdruck

23. Näheres zu ADSI Edit entnehmen Sie bitte Ihrer Windows-Server-Dokumentation

usw. Eine neue Zeile erhalten Sie mit Shift-Enter, einen neuen Absatz (zwei Zeilen) mit Enter.
Die Tokens *[VAR]* und *[/VAR]* sind case-sensitiv und müssen immer in Großbuchstaben geschrieben werden.



Die Variablen setzen den Inhalt des Wertes aus dem Active Directory ein. Schlägt die Auflösung der Variable fehl, so bleibt *[VAR]myvalue[/VAR]* unaufgelöst im Text stehen.

Die Ursachen können sein:

- Die Variable enthält keinen Wert
  (Information fehlt im Active Directory?)
- Die Variable existiert nicht (Schreibfehler?)
- Die Tokens *[VAR]* bzw. *[/VAR]* sind nicht in Großbuchstaben geschrieben (*[Var]* erzeugt einen Fehler!)

Soll eine allgemeingültige Information erscheinen, verwenden Sie eine Standardeinstellung, die Sie direkt im Trailertext eintragen und ändern können. Dieser Wert wird in die ausgehende Mail integriert. Schreiben Sie hinter die Variable ein Semikolon und direkt anschließend den für alle

Mitarbeiter gültigen Standardwert (siehe auch die fett markierten Werte im Screenshot oben). Beispiel:
[VAR]myvalue;HALLO[/VAR]

Wird also für *myvalue* kein Wert im Active Directory gefunden, so wird stattdessen *HALLO* verwendet.

Spezialfall: *[VAR]myvalue;[/VAR]*

Wenn Sie als Standardeinstellung eine leere Zeichenkette setzen, also hinter das Semikolon nichts eintragen, wird die Ausgabe der Variablen vollständig unterdrückt, falls aus dem Active Directory kein Wert entnommen werden kann.

Achten Sie darauf, dass sich das Active Directory immer auf dem aktuellen Stand befindet!

Kopieren Sie unseren vorkonfigurierten Trailer **Signatures**, den Sie in der Standard-Konfiguration vorfinden und passen Sie diesen für Ihre Zwecke an.

6. Aus der Registerkarte **Jobs** ersehen Sie, in welchen Jobs dieser Trailer verwendet wird.
7. Speichern Sie den Signatur-Trailer mit **OK**.

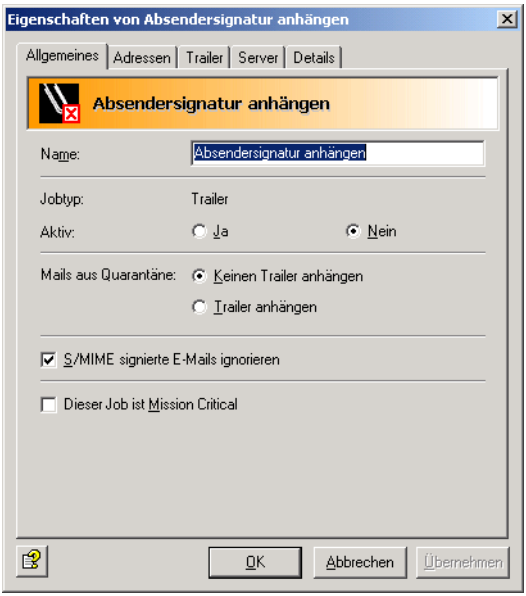
9.3.2 Individuelle Signaturen anhängen - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie den Job **Absendersignatur anhängen.** Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

9.3.2.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre

Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

Das heißt, in diesem Fall wird kein Trailer angehängt. Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

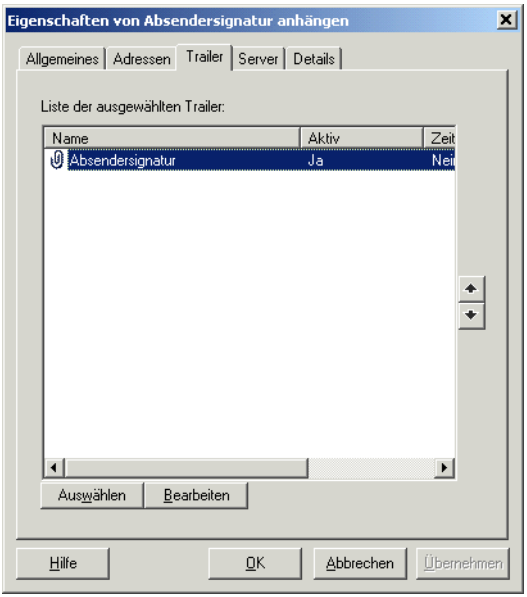
Dieser Job ignoriert Mails, die vom Client aus signiert (S/MIME-Signatur) versendet werden, da iQ.Suite Trailer die Mail öffnen muss, um den Textbaustein zu integrieren. Dadurch wird eine Signatur ungültig.

9.3.2.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in "Adresslisten" auf Seite 90.

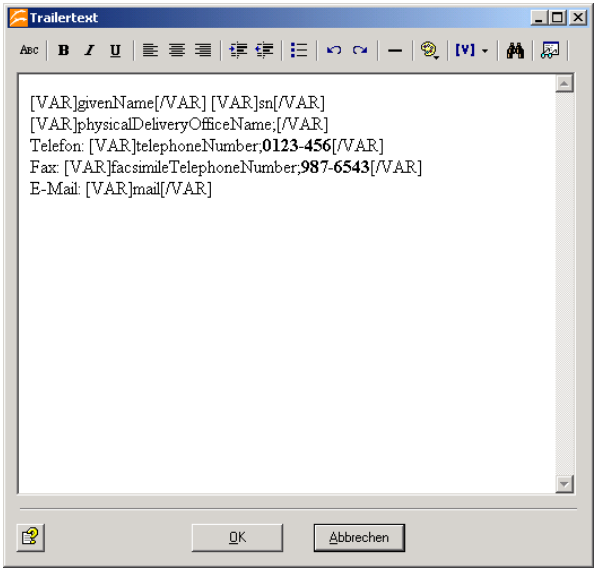
9.3.2.3 Trailer auswählen

Wählen Sie unter der Registerkarte **Trailer** den gewünschten Trailer aus.



Mit der Schaltfläche **Auswählen** können Sie einen anderen Trailer anhängen, sofern ein anderer Trailer angelegt worden ist. Für das Entfernen eines Trailers aus dem Job siehe "Trailer auswählen" auf Seite 198.

Die Standardkonfiguration enthält bereits einen vorkonfigurierten Trailer für eine **Absendersignatur**. Passen Sie diesen an Ihre eigenen Unternehmensrichtlinien an. Dazu klicken Sie auf **Bearbeiten** und anschließend auf die Registerkarte **Trailertext**. Dort erhalten Sie eine Vorschau des Textes. Klicken Sie auf **Bearbeiten**:



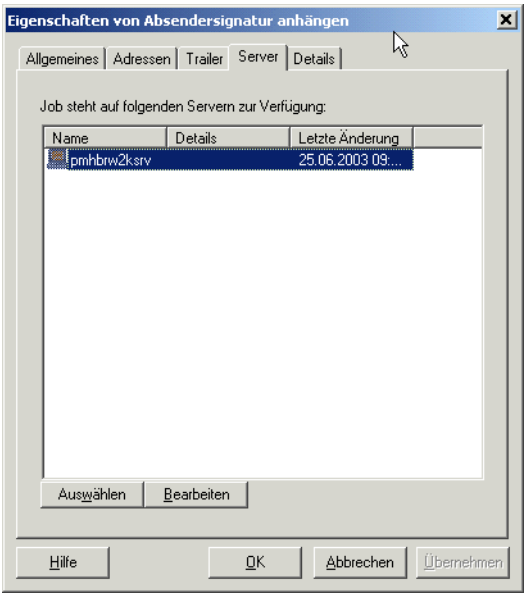
Passen Sie den Text an Ihre eigenen Unternehmensrichtlinien an und klicken Sie **OK**[24].

Sprechen Sie mit den Fachabteilungen über die Unternehmensrichtlinien und den Inhalt/Form der Trailer-Texte.

24. Zur Bearbeitung von Trailersignaturen siehe "Erstellen eines neuen Trailers für individuelle Signaturen" auf Seite 203.

9.3.2.4 Server auswählen

Auf der Registerkarte **Server** wählen Sie den oder die Server aus, auf denen der Job aktiv sein soll.



Klicken Sie auf die Schaltfläche **Auswählen**. Sie erhalten einen zu der Auswahl von Virenscannern analogen Dialog, siehe auch "Virenscanner auswählen" auf Seite 226.

Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein. Näheres zur Konfiguration von iQ.Suite Servern finden Sie in "Einstellungen für einen einzelnen iQ.Suite Server" auf Seite 85ff.

Da Sie einen Trailer nur an ausgehende Mails anhängen wollen, wählen Sie hier nur den Mailausgangsserver!

9.3.2.5 Details zum Job eingeben

Auf der letzten Registerkarte **Details** können Sie den Job näher beschreiben.

10 iQ.Suite Watchdog

10.1 Übersicht

Mit iQ.Suite Watchdog überprüfen Sie die E-Mails auf Viren, auf Typ und Größe eines Anhangs und auf die Gesamt-E-Mail-Größe.

Hierbei wird zwischen einer Prüfung auf der Transportebene (eingehende/ausgehende Nachrichten) und einer Prüfung in der MS Exchange Datenbank (öffentlicher und privater Informationsspeicher) unterschieden.

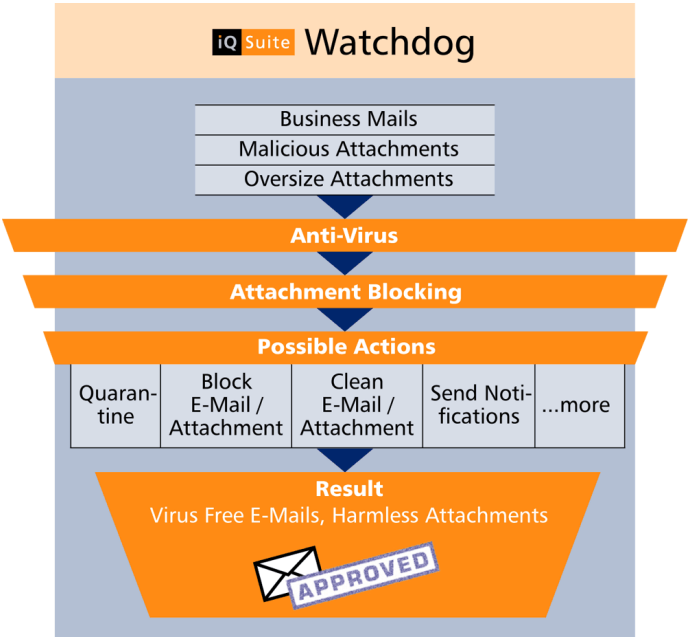
10.1.1 Jobtypen

- Virenprüfung ein- und ausgehender E-Mails
  Job: **Watchdog Virus Scanning**
- Virenprüfung in MS Exchange Datenbanken
  (on access & proactive/background)
  Job: **Informationsspeicher-Scan**
- Sperren von bestimmten Dateitypen im Anhang
  Job: **Watchdog Attachment Filtering**
- Beschränkung der E-Mail-Größe
  Job: **Watchdog E-Mail Size Filtering**
- Beschränkung von Typ und/oder Größe der Anhänge
  Job: **Watchdog Attachment/Size Filtering**

Legen Sie für jeden Einschränkungstyp einen separaten Job an! Die Jobtypen lassen sich später nicht mehr ändern.

Die genaue Vorgehensweise entnehmen Sie bitte den Beschreibungen ab “Virenprüfung einschalten - Jobbeispiel” auf Seite 224.

Grafisch dargestellt sieht die Arbeitsweise wie folgt aus:



10.2 Virenprüfung

10.2.1 ... ein- und ausgehender E-Mails

Die Virenprüfung erfolgt grundsätzlich durch einen oder auch mehrere Virenscanner von Fremdherstellern. Außer **AntiVir powered by H+BEDV** müssen diese Virenscanner vorher auf dem Exchange-Server installiert sein und werden von Watchdog aufgerufen und gestartet. Die Virenscanner müssen daher für Watchdog konfiguriert werden. Rufen Sie die **Basis-Konfiguration --> Utility-Einstellungen** auf und stellen Sie dort unter **Virenscanner** Ihre Virenscanner ein. Dieser Menüpunkt ist die Schnittstelle zwischen dem Virenscanner und iQ.Suite Watchdog. Die genaue Vorgehensweise für die Konfiguration finden Sie in “Virenscanner konfigurieren” auf Seite 216.

iQ.Suite Watchdog unterstützt Virenscanner der folgenden Hersteller:

- H+BEDV
- Sophos
- Norman
- Trend Micro

- Symantec
- McAfee
- F-Secure
- Command Software

Der **Watchdog Virus Scanning** Job startet gemäß der konfigurierten Bedingungen die ausgewählten Virenscanner. Die Bedingungen bestimmen, für welche E-Mails ein Job ausgeführt wird. Sind mehrere Virenscanner ausgewählt, so werden die E-Mails von allen Scannern auf Viren geprüft, ggf. gereinigt und weitere vorher definierte Aktionen durchgeführt:

Hier ein Beispiel für die Arbeitsweise eines Jobs für die Virenprüfung. Der Job prüft z.B. eine E-Mail mit dem Ergebnis: Virus gefunden. Daraufhin wird Virenalarm ausgelöst und eine Reihe von Aktionen in Gang gesetzt, die Sie selbst unter Aktionen definieren können. Sie können z.B. Folgendes festlegen:

1. Wenn ein Virus gefunden wird, soll die Originalmail gereinigt und dann dem Empfänger zugestellt werden.
2. Wenn die Originalmail nicht gereinigt werden kann, wird die betroffene E-Mail in den von Ihnen gewählten Ordner (Quarantäne) kopiert, das Original gelöscht und nicht zugestellt.
3. In diesem Fall werden Nachrichten an Administrator, Absender und Empfänger erstellt, die mit den relevanten Informationen des Virenscanners und iQ.Suite Watchdog versehen sind.

Diese Aktionen sind möglich:

- Auf Viren prüfen
- Von Viren reinigen
- Zusatz im Betreff
- Gesamte Mail in Quarantäne kopieren
- Betroffene Anhänge aus E-Mail entfernen
- Betroffene E-Mail löschen und nicht zustellen
- Ausführen einer externen Anwendung
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen

- X-Header-Feld hinzufügen
- Mail umleiten

10.2.2 ... im Informationsspeicher

Neben der Virenprüfung auf Transportebene ist die iQ.Suite auch in der Lage, Daten im öffentlichen oder privaten Informationsspeicher von MS Exchange zu prüfen.

Mit dem Informationsspeicher-Scan werden drei Hauptbereiche abgedeckt:

- **On-Demand Scan**

  Versucht ein Client eine Nachricht zu öffnen, wird ein Vergleich durchgeführt, um sicherzustellen, dass der Textkörper und der Anhang von der aktuellen Virensignaturdatei überprüft wurden. Wenn der Inhalt nicht anhand der aktuellen Virensignaturdatei überprüft wurde, wird die entsprechende Nachrichtenkomponente vor der Weiterleitung an den Client dem Virenscanner übermittelt. On-Demand Scan ist der geläufigste Bereich, für welchen der Informationsspeicher-Scan gewählt wird.

- **Proaktiver Scan**

  Der proaktive Scan überprüft neue eintreffende Nachrichten, bevor der Zugriff eines Clients über den On-Demand Scan erfolgt. Der proaktive Scan stellt eine Ergänzung zum On-Demand Scan dar, welcher für einen schnelleren Clientzugriff sorgen kann.

- **Hintergrund Scan**

  Beim Hintergrund Scan kann ein kompletter Prüflauf durch alle Elemente des Informationsspeichers angestoßen werden. Diese Überprüfung kann für den öffentlichen und privaten Informationsspeicher getrennt aktiviert werden. Es werden hierbei alle Elemente erfasst, welche mit der aktuellen Virenscannersignaturdatei noch nicht geprüft wurden.

Neben der zeitgesteuerten Überprüfung wird der Hintergrund-Scan auch immer beim Laden der Datenbanken (z.B. Start des Servers) ausgeführt.

Beim Informationsspeicher-Scan handelt es sich um eine serverweite Einstellung. Daher ist in der iQ.Suite immer ein Informationsspeicher-Scan Job pro Server verfügbar und nicht beliebig viele wie beim Watchdog Virus Scanning.

Wird in einer Nachricht ein Virus gefunden, lassen sich verschiedene Aktionen durchführen, die speziell auf den Informationsspeicher-Scan abgestimmt sind:

- **Objekt blocken**

  Das Blockieren verbietet den Zugriff auf das gesamte Nachrichtenobjekt. Bei aktuellen Microsoft E-Mail Clients wird beim Versuch, eine solche Nachricht zu öffnen, eine entsprechende Meldung generiert. Bei anderen/älteren E-Mail-Clients kann es zu unterschiedlichen Rückmeldungen kommen. Die blockierten Nachrichten können allerdings jederzeit über den Client gelöscht werden.

- **Ersetzen**

  Das Ersetzen tauscht das virulente Element der Nachricht (z.B. Dateianhang) durch einen Textvermerk aus. Das virulente Element wird gelöscht.

- **Nicht als virulent markieren**

  In Ausnahmefällen kann entschieden werden, dass bei einem gefundenen Virus das entsprechende Element nicht als virulent markiert wird. Nachfolgende Virenprüfungen werden das Element dann wiederum als virulent erkennen. Diese Aktion ist nur in Testumgebungen sinnvoll, da hier kein Schutz des Anwenders gewährleistet ist.

Die Virenprüfung des MS Exchange Informationsspeichers erfolgt über die Microsoft Virus Scanning API 2.0/2.5. Weitere Informationen hierzu finden Sie unter http://support.microsoft.com/kb/285667/DE/

Bei Nachrichten, die durch den Informationsspeicher-Scan blockiert werden, kann es zu Fehlermeldungen bei Datensicherungen des Informationsspeichers kommen.

Das Beenden oder Deinstallieren der iQ.Suite sowie das Anhalten des Informationsspeicher-Scan-Jobs deaktiviert nicht nur den aktiven Virenschutz des Informationsspeichers, sondern hebt auch die oben angesprochene Blockierung virulenter Inhalte auf.

10.2.3 Virenscanner konfigurieren

Alle Virenscanner außer AntiVir von H+BEDV werden nicht von uns ausgeliefert und müssen bereits vor der Installation der iQ.Suite auf Ihrem Server installiert sein (siehe auch "Installation der Virenscanner" auf Seite 25.) Die iQ.Suite ruft den Virenscanner durch das sogenannte **GROUP AV Interface**[25] - eine DLL-Datei - auf.

Deaktivieren Sie in jedem Fall eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virenscanner für das Verzeichnis `..\iQ.Suite\GrpData`!

Möchten Sie den AntiVir Virenscanner nicht oder nur zusätzlich verwenden, so gehen Sie bitte folgendermaßen vor:

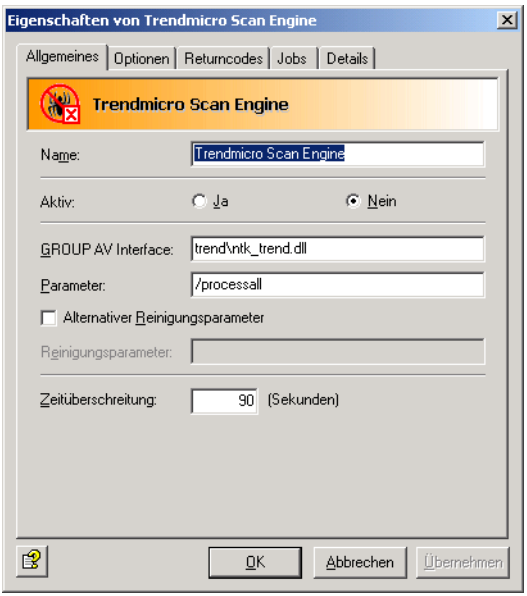
1. Installieren Sie den gewünschten Virenscanner. Vergewissern Sie sich, dass die iQ.Suite diesen Virenscanner unterstützt (siehe die Liste in "Virenprüfung" auf Seite 212). Sollte Ihr Virenscanner sich nicht in der Liste befinden, kontaktieren Sie bitte unseren Support.
2. Rufen Sie die Virenscanner-Konfiguration auf: **Basis-Konfiguration --> Utility-Einstellungen --> Virenscanner**.
3. Aktivieren Sie Ihre(n) Virenscanner: Wählen Sie die Registerkarte **Allgemeines --> Aktiv --> Ja**. Alternativ können Sie mit der rechten Maustaste den Virenscanner unter **Alle Tasks Aktivieren** bzw. **Deaktivieren**.
4. Tragen Sie in den entsprechenden Feldern in den Registerkarten **Allgemeines** und **Optionen** die Werte für Ihren Virenscanner ein. Beachten Sie dabei die Beschreibung für Ihren Virenscanner unter "Virenscanner konfi-

25. GROUP Anti Virus Interface = GAVI

gurieren" auf Seite 216. Entnehmen Sie die Bedeutung der einzelnen Parameter der Dokumentation Ihres Virenscanners.

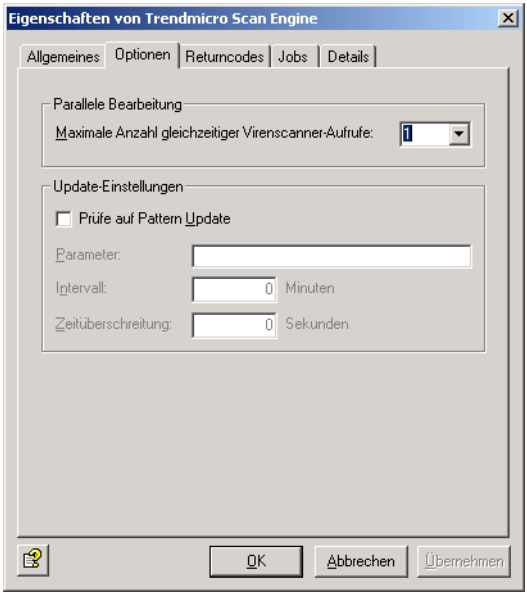
5. **Wenn Sie AntiVir nicht nutzen wollen:** Deaktivieren Sie diesen Virenscanner: Rufen Sie dazu mit einem Doppelklick die **Eigenschaften** von AntiVir auf und schalten Sie die Option **Aktiv** auf **Nein**.

Beispiel: Beim Trend Micro Virenscanner sieht das wie folgt aus:



Im Feld **GROUP AV Interface** muss der Name der GROUP Anti Virus Interface-DLL eingetragen sein. Diese ist für jeden Virenscanner vorkonfiguriert.

Unter **Optionen** erhalten Sie folgende Einstellungen:



- **Maximale Anzahl gleichzeitiger Virenscanner-Aufrufe:**
  bestimmt, wie viele Mails gleichzeitig durch diesen Virenscanner bearbeitet werden sollen. Die Anzahl sollte kleiner oder gleich mit der Einstellung in **iQ.Suite Server --> Eigenschaften -->** Registerkarte **Allgemeines: Anzahl der Threads** sein. Beispiel: Wenn Sie auf dieser Registerkarte die maximale Anzahl der Aufrufe auf 3 einstellen, so sollte die gleiche oder eine höhere Anzahl im Feld **Anzahl der Threads** angegeben sein. Siehe auch “Einstellungen für einen einzelnen iQ.Suite Server” auf Seite 85.

- **Update-Einstellungen**
  Die Update-Einstellungen benötigen Sie nur für den Trend Micro und den McAfee Virenscanner. Für alle anderen Virenscanner wird das Update automatisch durchgeführt.

- **Prüfe auf Pattern Update**

  Aktivieren Sie diesen Schalter, wenn Sie den **Trend Micro** oder **McAfee** Virenscanner einsetzen.

- **Parameter:**

  Geben Sie hier den vollständigen und absoluten Pfad in Anführungszeichen zum Pattern-Ordner des Virenscanners an, in den die Updates der Pattern abgelegt werden.

- **Intervall:**

  Zeitintervall in Minuten, in dem nach Pattern Updates gesucht wird. Minimalwert: 15 min.

- **Zeitüberschreitung:**

  Bei Zugriff auf den Server in Sekunden. Minimalwert: 60 Sekunden. Wir empfehlen eine Einstellung von 60 bis 120 Sekunden.

Die Bedeutung der **Returncodes** finden Sie unter **Details --> Anmerkungen**.

Aus der Registerkarte **Jobs** ersehen Sie, in welche Jobs der Virenscanner eingebunden ist.

Die Besonderheiten in der Konfiguration der einzelnen Virenscanner:

10.2.3.1 AntiVir Engine powered by H+BEDV

Die AntiVir Engine wird automatisch gefunden. Aktivieren Sie nur den Scanner.

Voreingestellte Parameter:
/decomp (entpacke PKLite und LZExe)
/verbosescan (prüfe komplette Datei)

Alternative Parameter:
/paranoid (interpretiere Warnung der heuristischen Analyse als Virus)

Wenn Sie einen Proxy-Server verwenden, passen Sie die **savapi.ini** für die Online-Updates der Virenpattern an:

1. Stoppen Sie den SAVAPI-Service.
2. Öffnen Sie das Verzeichnis `iQ.Suite\Engine\`.
3. Öffnen Sie die **savapi.ini**-Datei mit Notepad und setzen Sie folgende Parameter:

- Proxy-Server für Updates verwenden:
  Falls dieser Wert aktiviert (1) ist, versucht die Engine die Update-Downloads über den angegeben Proxy zu machen. In der Standard-einstellung wird kein Proxy-Server verwendet. Beispiel: ProxyEnab-led=0 (=nicht aktiviert).

- Adresse des Proxy-Servers:
  Hier kann der vollständige Name oder die IP-Adresse des für die Updates zu verwendenden Proxy-Servers eingetragen werden. Dieser Wert wird nur dann beachtet, wenn "ProxyEnabled" aktiviert ist.
  Beispiel: ProxyUrl=proxy.mydomain.de

- Proxy-Port-Adresse:
  Der in diesem Wert angegebene Port wird für die Kommunikation mit dem Proxy-Server bei einem Update verwendet. Dieser Wert wird nur dann beachtet, wenn "ProxyEnabled" aktiviert ist. Hier ist die Portnum-mer des Proxy-Servers einzutragen.
  Beispiel: ProxyPort=3128

- Username für Proxy-Server (Proxy-Authentifizierung)
  Hier wird der Benutzername eingetragen, unter dem sich der Update-Dienst am Proxy-Server anmelden soll. Dieser Wert wird nur dann beachtet, wenn "ProxyEnabled" aktiviert ist.
  Beispiel: ProxyUserName=fmaier

- Passwort für Proxy-Server (Proxy-Authentifizierung):
  Hier wird das Passwort eingetragen, mit dem sich der Update-Dienst zusammen mit dem Benutzernamen am Proxy-Server authentifizieren soll. Dieser Wert wird nur dann beachtet, wenn "ProxyEnabled" akti-viert ist.
  Beispiel: ProxyPassword=passwort

- Intervall für die Suche nach neuen Updates
  Dieser Wert gibt an, nach wie vielen Minuten der Update-Dienst nach neuen Versionen auf dem unter UpdateURL angegeben Server suchen soll. Die Zeit wird in Minuten angegeben. Der Standardwert ist alle 120 Minuten (2 Stunden). Die Engine wird direkt nach der ersten

Aktion (Virensuche) automatisch ein Update der Engine und der Virensignaturen durchführen. Ist dieser Wert 0, wird die automatische Suche nach neuen Updates deaktiviert.
Beispiel: UpdateInterval=120

10.2.3.2 Command Software Scan Engine

Alle ***.def** Dateien (von command com) und **english.txt** müssen sich im selben Verzeichnis befinden wie die **ntk_css.dll**. Kopieren Sie die **ntk_css.dll** in das Installationsverzeichnis von Command und überprüfen Sie das Vorhandensein aller anderen Dateien. Der vollständige Installationspfad der GROUP Anti Virus Interface-DLL muss im Feld **GROUP AV Interface** eingetragen sein (aus der Serversicht). Beispiel:

```
c:\program files\CommandCom\ntk_css.dll
```

Parameter: */nodecomp* (keine Komprimierung)

10.2.3.3 F-Secure Scan Engine

Die IP-Adresse (oder der Hostname) und die Portnummer des F-Secure-Servers müssen als Parameter übergeben werden. Der Standard Port ist 18971.

Format des Parameters: IP-Adresse:Portnummer

z.B.: 192.168.0.1:18971
oder host.name:18971

10.2.3.4 McAfee Scan Engine

1. Bei der Installation wird im iQ.Suite Verzeichnis der Ordner `\bin\mcafee` angelegt. Kopieren Sie die McAfee-DLL (**mcscan32.dll**) und die Dateien **internet.dat**, **scan.dat**, **names.dat** und **clean.dat** in dieses Verzeichnis.
2. Aktivieren Sie das **Pattern Update** in der **Basis-Konfiguration --> Virenscanner**, Registerkarte **Optionen**. Tragen Sie außerdem den Pfad des Pattern Verzeichnisses von McAfee als **Parameter** ein. Setzen Sie den Pfad in Anführungszeichen!

Parameter:

-maliciousapplications
Einige weitverbreitete Anwendungen (wie Passwort-Knacker) können böswillig

eingesetzt werden bzw. eine Sicherheitsbedrohung darstellen. Beim Setzen dieses Parameters sucht der Virenscanner auch nach dieser Art von Dateien.

-notscanforjokes
„Jokes“ (=Witze) nicht prüfen. Das Prüfen von als Witze klassifizierten Dateien kann mit diesem Parameter abgeschaltet werden.

-noheuristicanalysis
Die heuristische Analyse [Suche nach ähnlichen Mustern (d.h. nach potenziellen Viren)] ermöglicht das Finden neuer, bisher unbekannter Viren, was allerdings die Performance des Systems beeinträchtigen kann - mit diesem Parameter kann man die heuristische Analyse ausschalten.

-notdecompress
Der interne Entpacker des Virenscanners wird ausgeschaltet.

McAfee kann außerdem

- Einzelne Dateien oder komplette Verzeichnisse prüfen
- Archive (ARJ, ZIP, LHARC) prüfen
- Einen Returncode bei passwortgeschützten Dateien ausgeben

Bekannte Probleme:

- Bei einer nicht zu reinigenden Datei wird die Rückmeldung "Virus gefunden" ausgegeben, obwohl die Datei gelöscht wird.
- Als ZIP gepackte virulente Dateien werden zwar gereinigt aber es wird trotzdem ein Virus zurückgemeldet; erst ein erneuter Virenscan liefert OK zurück.
- Als ARJ gepackte virulente Dateien werden nicht gereinigt, die Viren werden aber erkannt.

10.2.3.5 Norman Scan Engine

Die Norman Scan Engine wird automatisch gefunden. Aktivieren Sie nur den Scanner.

Parameter:
/nodecomp (komprimierte Dateien nicht prüfen)

/norecursion (komprimierte Dateien innerhalb von komprimierten Dateien nicht prüfen)

10.2.3.6 Sophos Scan Engine (SAVI)

Der Sophos Virenscanner wird automatisch gefunden. Aktivieren Sie nur den Scanner.

10.2.3.7 Symantec Scan Engine

Der Symantec Virenscanner wird automatisch gefunden. Aktivieren Sie nur den Scanner.

Bekannte Probleme bei Symantec Scan Engine Version 3.0:

- Schreibgeschützte Dateien werden nicht geprüft, sondern es wird nur ein Fehler zurückgegeben.
- Verschlüsselte Dateien werden weder geprüft noch gereinigt, der Returncode ist trotzdem 0 (wie für OK).

Voreingestellte Parameter:
Die IP-Adresse (oder der Hostname) und die Portnummer des Symantec Carrier-Scan Servers müssen als Parameter übergeben werden. Der Standard Port ist 7777.

Format: IP-Adresse:Portnummer

z.B.: 192.168.0.1:7777
oder host.name:7777

10.2.3.8 Trend Micro Scan Engine

1. Bei der Installation wird im iQ.Suite Verzeichnis der Ordner `\bin\trend` angelegt. Kopieren Sie die Trend Micro DLL (**vsapi32.dll**) und die Dateien **lpt$vpn.*** in dieses Verzeichnis.
2. Aktivieren Sie das **Pattern Update** in der **Basis-Konfiguration --> Virenscanner**, Registerkarte **Optionen**. Tragen Sie außerdem den Pfad des Pattern Verzeichnisses von Trend Micro als **Parameter** ein. Setzen Sie den Pfad in Anführungszeichen!

Voreingestellte Parameter:
/processall (prüfe alle Dateien)
/smartdecomp (aktiviere „Smart“-Komprimierung)

Alternative Parameter:

/nodecomp (Komprimierte Dateien nicht prüfen)

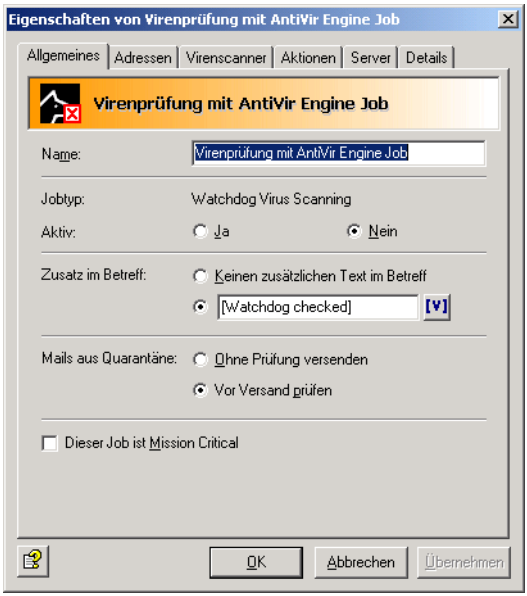
/norecursion (komprimierte Dateien innerhalb von komprimierten Dateien nicht prüfen)

10.2.4 Virenprüfung einschalten - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Mail Transport Jobs** finden Sie den Job **Virenprüfung mit AntiVir Engine**. Öffnen Sie diesen mit einem Doppelklick.

10.2.4.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Watchdog checked**. Dieser Zusatz wird in den Betreff jeder Mail eingefügt, die virenfrei ist.

Dieser Job bearbeitet auch diejenigen Mails, die aus der **Quarantäne** wieder versendet werden. Die **Sende-Option** beim Versand aus der Quarantäne ist Job-übergreifend und hat Priorität. Wenn Sie eine Mail also mit der Quarantäne-Sende-Option **Zustellen ohne weitere iQ.Suite Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die **Sende-Option** deshalb auf **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen**.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in "Aus Quarantäne senden" auf Seite 130.

Dieser Job ist Mission Critical

Ein Job ist **Mission Critical**, wenn die Mail bei einem Verarbeitungsfehler - wie beispielsweise bei fehlendem Virenscanner - in den Bad-Mail-Bereich abgelegt werden soll. Wählen Sie diese Option für unternehmenskritische Jobs wie Virenprüfungen (Haken wird gesetzt).

Solange der Verarbeitungsfehler nicht behoben ist, wird bei dieser Option **jede** E-Mail - eingehend oder ausgehend - in den Bad-Mail-Bereich überführt!

Ein Job ist **nicht Mission Critical**, wenn das Ergebnis des Jobs im Falle eines Verarbeitungsfehlers bei der betreffenden Mail ignoriert werden soll. Die Mail wird in diesem Fall dem nächsten Job zur Bearbeitung übergeben. Jeder Verarbeitungsfehler wird im Windows Event Log eingetragen. Tritt der Verarbeitungsfehler fünf Mal hintereinander auf, wird der Job deaktiviert. Der deaktivierte Job wird nach 15 Minuten automatisch wieder gestartet. Wählen Sie diese Option für nicht unternehmenskritische Jobs wie das Anhängen einer individuellen Signatur durch iQ.Suite Trailer (Haken wird nicht gesetzt).

Die Standardeinstellung für alle Jobs ist **nicht Mission Critical**. Welche Jobs als unternehmenskritisch gelten, sollte in den Firmenrichtlinien festgelegt werden.

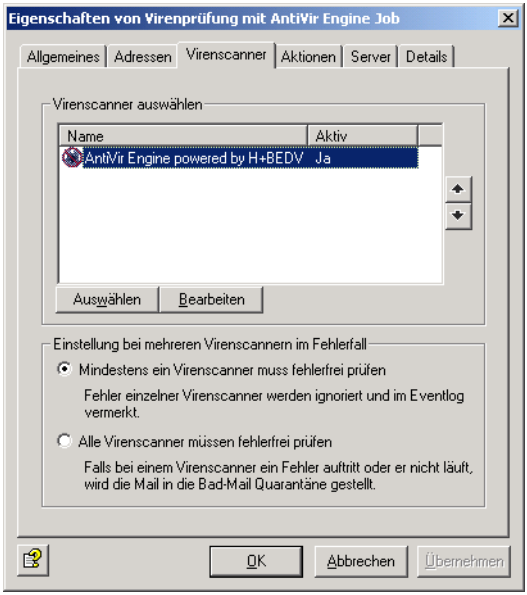
10.2.4.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhan-

denen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

10.2.4.3 Virenscanner auswählen

Wählen Sie auf der Registerkarte **Virenscanner** durch die Schaltfläche **Auswählen** die von Ihnen eingesetzten Virenscanner aus. Die Standardeinstellung ist die AntiVir Engine. Die Reihenfolge der zu verwendenden Virenscanner können Sie mit Hilfe der Pfeiltasten (hoch und runter) verändern, wenn Sie mehrere Virenscanner ausgewählt haben.



Wenn Sie mehrere Virenscanner einsetzen, wählen Sie aus, ob nur einer oder alle eingesetzten Virenscanner erfolgreich prüfen müssen.

Diese Option ist unabhängig vom Ergebnis der Prüfung und betrifft nur die Einsatzfähigkeit der Virenscanner. Sollte ein Virenscanner eine Mail als infiziert erkennen, so wird diese Mail auf keinen Fall an den Empfänger gesendet, wenn Sie unter **Aktionen „Lösche E-Mail“** konfiguriert haben!

Mindestens ein Virenscanner muss fehlerfrei prüfen

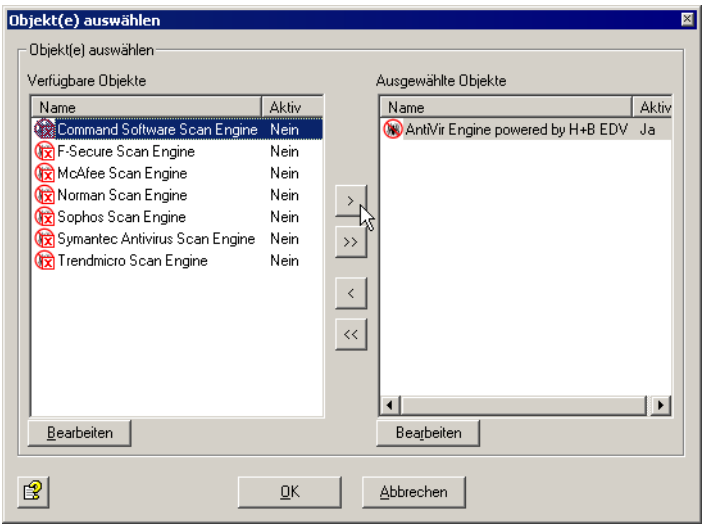
Es genügt, wenn einer der eingesetzten Virenscanner die Mail fehlerfrei prüft und als virenfrei erkennt. Wenn andere konfigurierte Virenscanner ausfallen sollten, wird die Mail an den Empfänger gesendet, obwohl sie noch nicht durch alle Virenscanner geprüft worden ist.

Alle Virenscanner müssen fehlerfrei prüfen

Alle eingesetzten Virenscanner müssen die Mail fehlerfrei prüfen und als virenfrei erkennen. Sollte einer der konfigurierten Virenscanner ausfallen oder abgeschaltet sein und deswegen die Mail nicht prüfen können, wird die Mail in die Bad-Mail-Quarantäne überführt.

Die Standard- und empfohlene Einstellung ist **Mindestens ein Virenscanner muss fehlerfrei prüfen**.

Klicken Sie nun auf die Schaltfläche **Auswählen**. Sie erhalten folgenden Dialog:



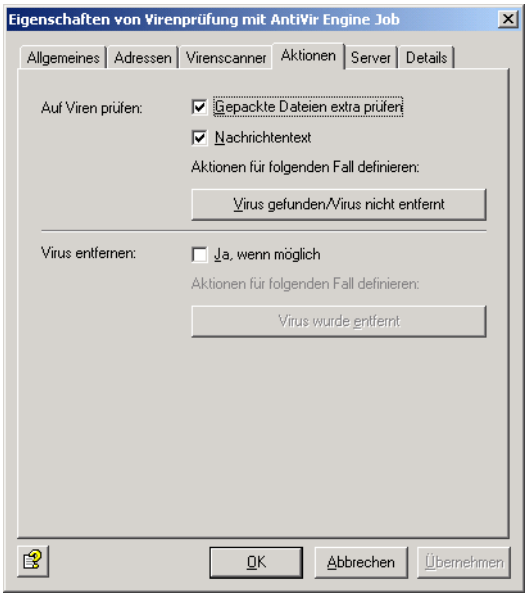
Sie können mehrere Virenscanner auswählen. Markieren Sie die gewünschten Virenscanner und verschieben Sie sie mit den Pfeiltasten in das rechte, zum Entfernen in das linke Fenster. Ausgewählt sind die Virenscanner im rechten Fenster. Alternativ können Sie die Virenscanner mit einem Doppelklick von der linken

auf die rechte Seite (und umgekehrt) verschieben. Die Basis-Konfiguration eines markierten Virenscanners lässt sich mit **Bearbeiten** aufrufen.

Damit der Virenscanner korrekt arbeiten kann, muss er vorher installiert, konfiguriert und aktiv gesetzt worden sein. Sie können im **iQ.Suite Monitor -->** <Server> --> **Server Status** (im rechten Fensterbereich) unter der Registerkarte **Virenscanner-Test** die Funktionalität prüfen. Näheres zur Konfiguration von Virenscannern finden Sie in "Virenscanner konfigurieren" auf Seite 216.

10.2.4.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine virenverseuchte Mail gefunden hat:



Dieser Job soll die Mail auf Viren prüfen, aber nicht versuchen, die Mail bzw. den Anhang von diesen Viren zu reinigen. In der Regel sind zwar alle Virenscanner zu einer Reinigung in der Lage. Da es in der Praxis aber kaum noch vorkommt, dass Viren versehentlich von bekannten Kommunikationspartnern versendet werden,

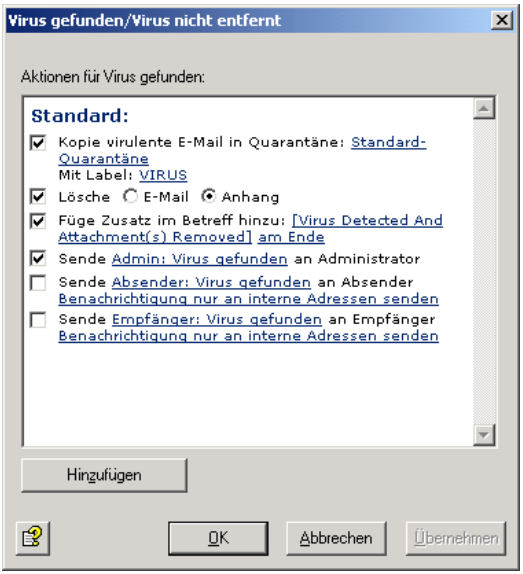
sondern es meist Spam ist, der gleichzeitig Viren enthält, ist es effektiver, virenbehaftete Anhänge sofort in die Quarantäne zu stellen.

Gepackte Dateien extra prüfen: Sollten Sie einen Virenscanner einsetzen, der keinen integrierten Entpacker besitzt, schalten Sie diese Option an. Damit wird ein interner Entpacker die gepackten Dateien zunächst extrahieren und danach einzeln dem Virenscanner zuführen.

Nachdem Sie festgelegt haben, was genau geprüft werden soll, definieren Sie zwei unterschiedliche Aktionen:

1. Für den Fall, dass ein Virus gefunden wurde und die Datei nicht erfolgreich gereinigt werden konnte,
2. für den Fall, dass die Reinigung der Datei erfolgreich verlaufen ist und der Virus entfernt wurde (falls Sie diese Option ausgewählt haben).

Für den ersten Fall sehen die Aktionen wie folgt aus:


Virus gefunden/Virus nicht entfernt
Aktionen für Virus gefunden:
Standard:
Kopie virulente E-Mail in Quarantäne: Standard-Quarantäne
Mit Label: VIRUS
Lösche E-Mail Anhang
Füge Zusatz im Betreff hinzu: [Virus Detected And Attachment(s) Removed] am Ende
Sende Admin: Virus gefunden an Administrator
Sende Absender: Virus gefunden an Absender
Benachrichtigung nur an interne Adressen senden
Sende Empfänger: Virus gefunden an Empfänger
Benachrichtigung nur an interne Adressen senden
Hinzufügen
OK
Abbrechen
Übernehmen

Eine Kopie der Mail wird in die Quarantäne gestellt und die betroffenen Anhänge werden gelöscht. Das beinhaltet, dass die Mail nur dann an den Empfänger zugestellt wird, wenn der Nachrichtentext virenfrei war und der Anhang gelöscht werden konnte. Eine Benachrichtigung über den Virus wird an den Administrator

versandt. Diese Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

Prüfen Sie, ob an Ihr Unternehmen gesendeten Virenmails sehr häufig gleichzeitig Spam sind. Wenn das der Fall ist, löschen Sie am besten sofort die gesamte E-Mail und nicht nur den Anhang. So müssen die übrig gebliebenen Nachrichtentexte nicht noch auf Spam untersucht werden.

Wenn Sie die Option **Auf Viren prüfen: Nachrichtentext** aktiviert haben und tatsächlich ein Virus im Text gefunden wird, so wird die gesamte E-Mail inklusive der Anhänge gelöscht, wenn Sie **Lösche Anhang** gesetzt haben (es wird kein Anhang ohne Nachrichtentext zugestellt). Der betroffene Mailabschnitt wird in der Regel einzeln gelöscht. Wenn nur der Anhang virulent war, wird auch nur dieser gelöscht.

Klicken Sie auf die Schaltfläche **Hinzufügen**, falls Sie weitere Aktionen definieren wollen:

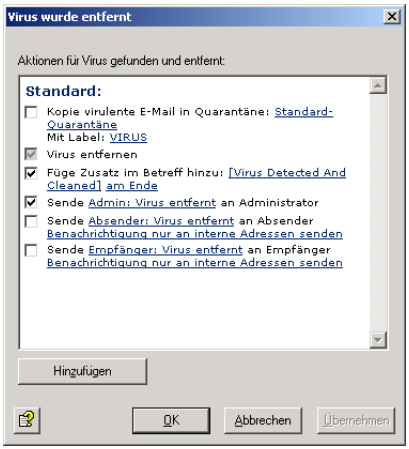
Anmerkung zu **Mail umleiten**: Wenn Sie eine TNEF-Mail an eine externe Adresse umleiten, erhalten Sie dort eine leere Mail, evtl. mit einem **winmail.dat** Anhang. Das TNEF-Format wird von Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine E-Mail sendet. Bei der Kommunikation über das Internet bzw. bei der Verwendung von anderen E-Mail Programmen wird dieses Format nicht verwendet.

Wählen Sie **Benachrichtigung** für eine Benachrichtigung an einen selbst zu definierenden Empfänger oder **Starte externe Anwendung**, um ganz andere Aktionen durchzuführen und klicken Sie auf **Weiter**:

Klicken Sie auf das Symbol für das Adressbuch , um weitere Empfänger auszuwählen oder **eigene Adressen** zu definieren. Klicken Sie auf **Fertigstellen**, wenn der Empfänger eingetragen ist.

Für den Start einer externen Anwendung geben Sie den Pfad, die optionalen Parameter und eine Zeitüberschreitung an:

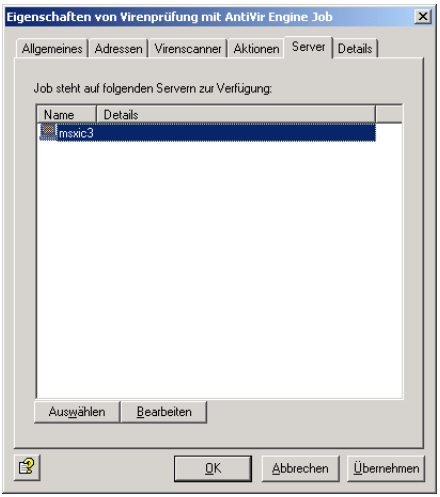
Für den zweiten Fall - Virus wurde entfernt - sehen die Aktionen wie folgt aus:


Virus wurde entfernt
Aktionen für Virus gefunden und entfernt:
Standard:
Kopie virulente E-Mail in Quarantäne: Standard-Quarantäne
Mit Label: VIRUS
Virus entfernen
Füge Zusatz im Betreff hinzu: [Virus Detected And Cleaned] am Ende
Sende Admin: Virus entfernt an Administrator
Sende Absender: Virus entfernt an Absender
Benachrichtigung nur an interne Adressen senden
Sende Empfänger: Virus entfernt an Empfänger
Benachrichtigung nur an interne Adressen senden
Hinzufügen
OK
Abbrechen
Übernehmen

Die E-Mail wird zugestellt, ein Zusatz im Betreff eingefügt und eine Benachrichtigung an den Administrator geschickt, damit dieser Vorgang nachvollzogen werden kann.

10.2.4.5 Server auswählen

Auf der Registerkarte **Server** wählen Sie den oder die Server aus, auf denen der Job aktiv sein soll.

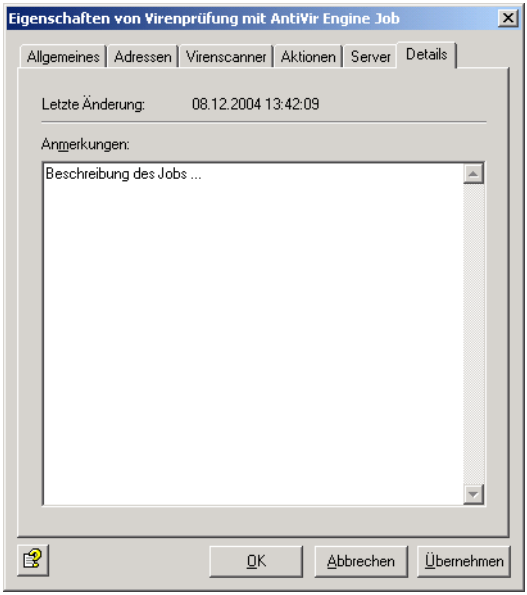


Klicken Sie auf die Schaltfläche **Auswählen**. Sie erhalten einen zu der Auswahl von Virenscannern analogen Dialog.

Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein. Näheres zur Konfiguration von iQ.Suite Servern finden Sie in “Einstellungen für einen einzelnen iQ.Suite Server” auf Seite 85ff.

10.2.4.6 Details zum Job eingeben

Auf der letzten Registerkarte **Details** können Sie den Job näher beschreiben:



10.3 Virenprüfung im Informationsspeicher - Jobbeispiel

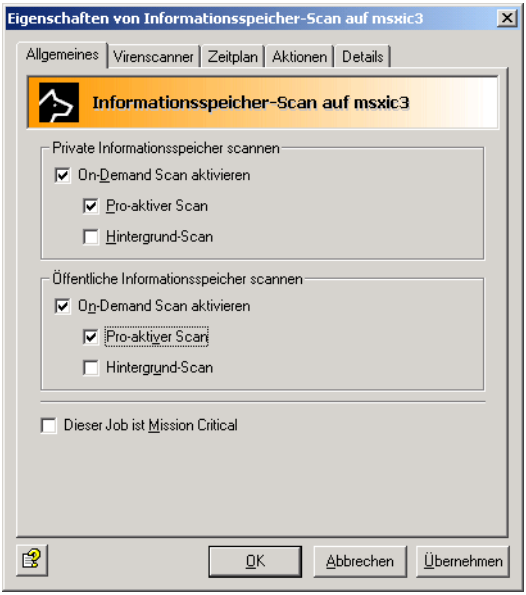
Unter **Richtlinien-Konfiguration** finden Sie im Bereich **Informationsspeicher-Jobs** pro Server einen **Informationsspeicher-Scan** Job. Öffnen Sie diesen mit einem Doppelklick.

Nach dem Aktivieren/Deaktivieren des Informationsspeicher-Scan Jobs kann es bis zu zwei Minuten dauern, bis der Exchange Store die Änderung registriert.

10.3.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie sowohl für den Privaten als auch für den Öffentlichen Informationsspeicher den On-Demand Scan aktivieren.

Zusätzlich zum On-Demand Scan können der Proaktive Scan und der Hintergrund-Scan aktiviert werden. Nähere Informationen dazu finden Sie in “... im Informationsspeicher” auf Seite 214.



Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

10.3.2 Virenscanner auswählen

Gehen Sie analog zur Beschreibung in “Virenscanner auswählen” auf Seite 226 vor.

10.3.3 Zeitplan festlegen

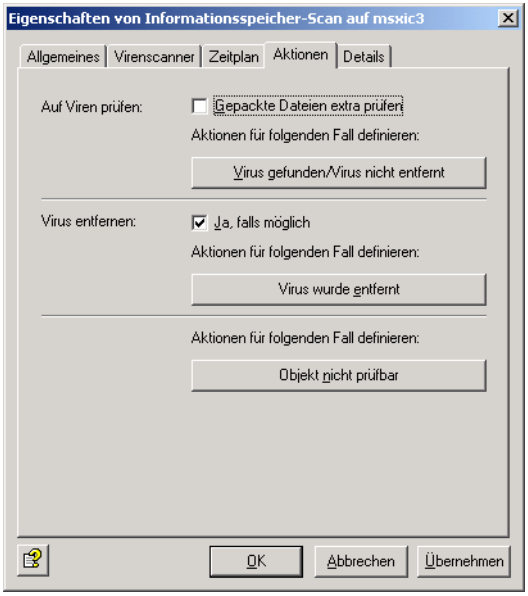
Auf der Registerkarte **Zeitplan** können Sie für den Neustart der Scans einen Zeitplan erstellen. Durch einen Neustart der Scans werden sämtliche Elemente im Informationsspeicher neu überprüft. Dieses betrifft alle drei Scanmodi. Falls Sie den Hintergrund-Scan aktiviert haben, kann diese Prüfung sehr zeit- und ressourcenintensiv sein. Es ist daher empfehlenswert, den Neustart zu Tagesrandzeiten und in Abhängigkeit der Virenscanneraktualisierung zu starten.

Um einen Eintrag im Zeitplan anzulegen, klicken Sie auf **Hinzufügen**. Wählen Sie anschließen die Startzeit und die Tage, an welchen der Neustart ausgeführt werden soll. Durch **OK** wird die Auswahl dem Zeitplan hinzugefügt:

10.3.4 Aktionen festlegen

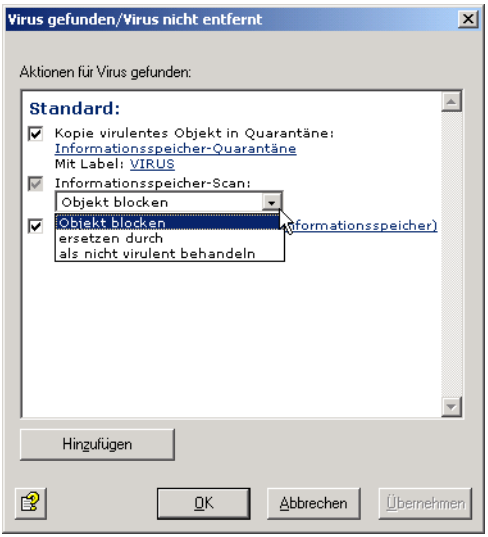
In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine virenverseuchte Mail gefunden hat.

Gepackte Dateien extra prüfen: Sollten Sie einen Virenscanner einsetzen, der keinen integrierten Entpacker besitzt, schalten Sie diese Option an. Damit wird ein interner Entpacker die gepackten Dateien zunächst extrahieren und danach einzeln dem Virenscanner zuführen.



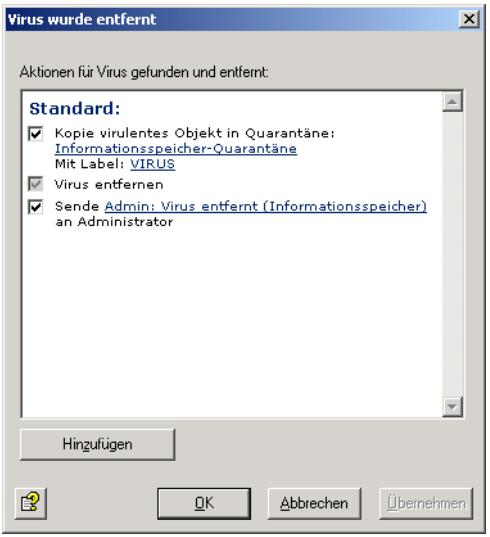
Es sind drei unterschiedliche Aktionen möglich:

1. **Virus gefunden/Virus nicht entfernt**: Behandelt den Fall, dass ein Virus gefunden wurde und die Datei nicht erfolgreich gereinigt werden konnte.



   a) Zunächst wählen Sie, ob eine Kopie des Objektes in eine Quarantäne gestellt und mit einem Label versehen werden soll. Für den Informationsspeicher-Scan steht eine spezielle Standardquarantäne zur Verfügung.
   b) Das Objekt kann mit der zweiten Option wahlweise geblockt, ersetzt oder ignoriert/nicht markiert werden. Siehe auch “... im Informationsspeicher” auf Seite 214.
   c) Mit der letzten Standardoption wählen Sie, ob eine Benachrichtigung an den/die Administrator/en versendet werden soll.
   d) Über die Schaltfläche **Hinzufügen** können Sie weitere Aktionen auswählen. So ist es beispielsweise möglich, Benachrichtigungen an beliebige Empfänger zu versenden oder eine externe Anwendung zu starten.

2. **Virus wurde entfernt**: Behandelt den Fall, dass die Reinigung der Datei erfolgreich verlaufen ist und der Virus entfernt wurde.

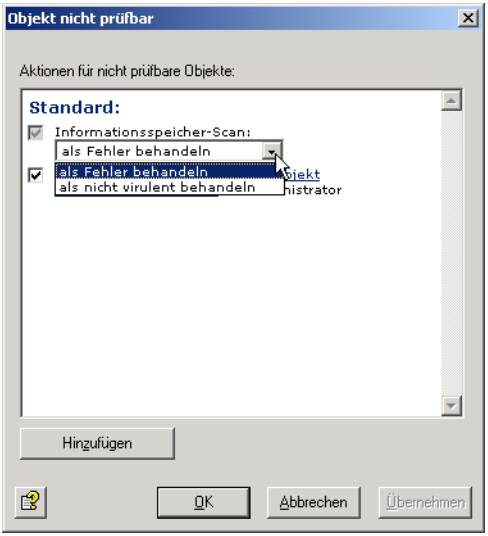


Hier können folgende Aktionen definiert werden:

a) Mit der ersten Option wählen Sie, ob eine Kopie des Objektes in eine Quarantäne gestellt und mit einem Label versehen werden soll. Die Kopie wird vor der Reinigung des Objektes erstellt, so dass sich das Objekt im Originalzustand in der Quarantäne befindet.

b) Zusätzlich können Sie wählen, ob eine Benachrichtigung an den/die Administrator/en versendet werden soll.

3. **Objekt nicht prüfbar**: Behandelt den Fall, dass die Dateien nicht geprüft werden konnten. So lässt sich beispielsweise das Verhalten der iQ.Suite beim Auffinden verschlüsselter Objekte beeinflussen, welche naturgemäß nicht einsehbar und damit auf Viren prüfbar sind.



Hier stehen Ihnen zwei Optionen zur Verfügung. Im Feld **Informations-speicher-Scan** können Sie das Objekt

a) **Als Fehler behandeln**

Das Objekt wird beim nächsten Scanvorgang erneut überprüft. Der Zugriff ist dabei blockiert, falls vorhergehende Scanvorgänge das Objekt nicht als virenfrei behandelt haben.

b) **Als nicht virulent behandeln**

Das Objekt wird behandelt, als wäre es virenfrei. Es wird erst beim nächsten Neustart der Virenprüfung erneut geprüft.

Des Weiteren ist es möglich, eine Benachrichtigung an den Administrator zu versenden, sowie mit **Hinzufügen** zusätzliche Aktionen auszuführen.

10.3.5 Job Details

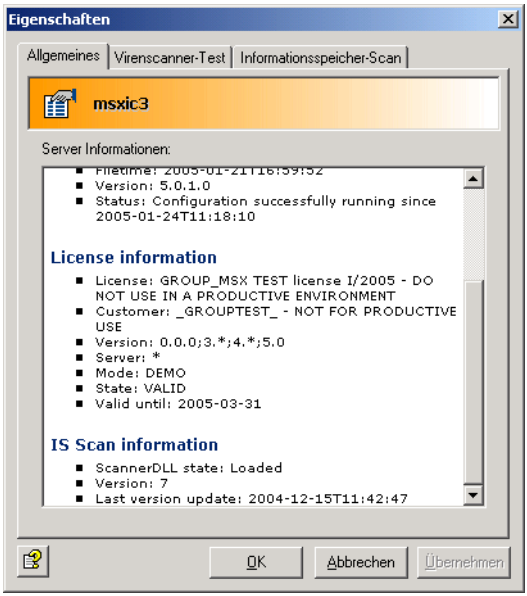
Die Eingabe der Job Details wird wie in der Beschreibung zu "Details zum Job eingeben" auf Seite 233 durchgeführt.

10.3.6 Server Status

Unter **iQ.Suite Monitor --> Server** --> <servername> befindet sich im rechten Fensterbereich der **Server Status**, mit dem Sie sowohl den aktuellen Status des

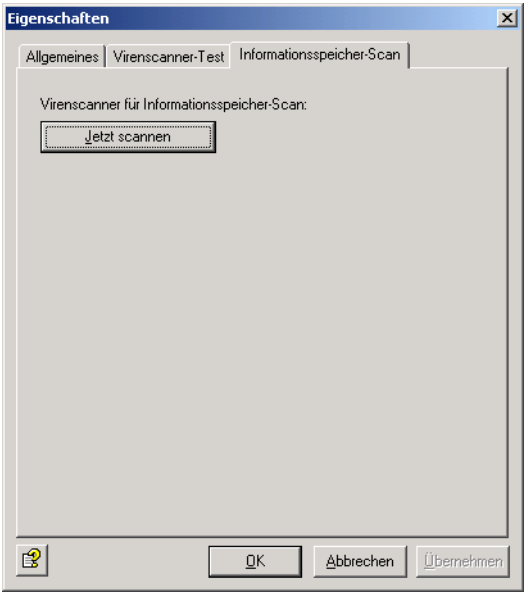
Informationsspeicher-Scans als auch die Option für einen manuellen Neustart finden.

Aus der Registerkarte **Allgemeines** ersehen Sie



- Ob die Scanner-DLL für den Informtionsspeicher-Scan geladen ist. Sobald die DLL **Loaded** anzeigt, ist der Informationsspeicher-Scan aktiv.
- Die Version des Informationsspeicher-Scans. Jeder Neustart erhöht diesen Wert.
- Wann die letzte Versionsaktualisierung erfolgte und Zeit und Datum des letzten Neustarts.

Auf der Registerkarte **Informationsspeicher-Scan** erhalten Sie die Möglichkeit, den Hintergrund-Scan neu zu starten:



Durch einen Neustart des Scans werden sämtliche Elemente im Informationsspeicher neu überprüft. Das betrifft alle drei Scanmodi. Falls Sie den Hintergrund-Scan aktiviert haben, kann diese Prüfung sehr zeit- und ressourcenintensiv sein. Es ist daher empfehlenswert, den Neustart zu Tagesrandzeiten und in Abhängigkeit der Virenscanneraktualisierung zu starten.

10.4 Dateieinschränkungen für den Anhang

Dateien können nach den Kriterien Typ und Größe eingeschränkt werden. Zunächst können Sie bestimmte Typen von Dateien nicht zulassen. Außerdem können Sie die maximale Größe einer E-Mail und die maximale Größe der Anhänge von E-Mails festlegen. Die Größe und der Typ der Anhänge können auch in einem gemeinsamen Job geprüft werden.

10.4.1 ... nach Typ

Die Datei muss von iQ.Suite Watchdog identifiziert werden. Dafür wird der Fingerprint[26] der Datei geprüft, der das binäre Dateimuster, z.B. bei *.exe-Dateien und/oder die Dateierweiterung (Extension), z.B. bei *.vbs-Dateien, enthält. Das

26. siehe hier “Fingerprints konfigurieren” auf Seite 243.

Ergebnis dieser Prüfung wird mit den verbotenen/erlaubten Fingerprints unter Watchdog-Einschränkungen verglichen und entsprechend ausgegrenzt oder durchgelassen. Für abgelehnte Dateien werden dann die Aktionen aus dem Job ausgeführt, z.B. bei einer E-Mail mit einem verbotenen Anhang:

1. Der verbotene Anhang wird in die Quarantäne kopiert.
2. Der Nachrichtentext wird dem Empfänger zugestellt.
3. Benachrichtigungen werden an den Administrator und den Absender geschickt.

Folgende Aktionen sind bei einem **Watchdog Attachment Filtering** Job möglich:

- Zusatz im Betreff
- Gesamte Mail in Quarantäne stellen
- Betroffene Anhänge aus der E-Mail entfernen
- Betroffene E-Mail löschen und nicht zustellen
- Eine externe Anwendung ausführen
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- X-Header-Feld hinzufügen
- Mail umleiten

10.4.2 ... nach E-Mail-Größe

E-Mails können anhand Ihrer Gesamtgröße analysiert und ggf. abgewiesen werden. Das Limit pro E-Mail können Sie unter der Registerkarte **E-Mail-Größe** einstellen.

Folgende Aktionen sind bei einem **Watchdog E-Mail Size Filtering** Job möglich:

- Zusatz im Betreff
- Gesamte Mail in Quarantäne stellen
- Betroffene E-Mail löschen und nicht zustellen
- Eine externe Anwendung ausführen
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen

- Andere, frei wählbare Personen benachrichtigen
- X-Header-Feld hinzufügen
- Mail umleiten

10.4.3 ... nach Typ und/oder Anhanggröße

E-Mails können anhand der Größe ihres Anhangs analysiert und ebenfalls abgewiesen werden. Die maximale Größe eines Anhangs pro E-Mail können Sie unter der Registerkarte **Fingerprint/Größe** einstellen. Es ist möglich, in diesem Job gleichzeitig den Typ des Anhangs einzuschränken.

Die Aktionsmöglichkeiten sind bei einem **Watchdog Attachment/Size Filtering** Job die gleichen wie in einem Attachment Filtering Job.

10.4.4 Fingerprints konfigurieren

Ein Fingerprint besteht aus einem Namensmuster und/oder einem Binärmuster.

- Namensmuster: Damit können Fingerprints anhand von Dateiname und -erweiterung (*.exe, ...) konfiguriert werden.
- Binärmuster: Damit können Fingerprints anhand von eindeutigen binären Dateiinformationen konfiguriert werden.

Mit dem Namensmuster sind natürlich auch Manipulationen möglich, da (wenn die Anwender davon wissen) einfach die Erweiterung geändert werden kann. Das Binärmuster ist eine eindeutige Zuordnung zu einem Format und lässt sich in der Datei nicht so leicht manipulieren. Somit ist der sichere Weg, ein Dateiformat zu erkennen, die Eingabe eines Binärmusters.

Mit Namensmustern ist es aber möglich, auf neue Virusattacken schnell zu reagieren:

Sobald bekannt ist, mit welchen Anhangnamen ein neuer Virus verbreitet wird (Beispiel: Nimda Virus = readme.exe) kann die Virusattacke abgewehrt werden, noch bevor ein Virus Pattern Update des Antivirus Herstellers verfügbar ist. Der Dateiname wird einfach mit dem Namensmuster als neuer Fingerprint angelegt.

Auch das Blocken individueller Dateien ist möglich:

Setzt ein Unternehmen Individualsoftware ein, welche ein eigenes Dateiformat erzeugt, kann dafür ebenfalls ein Fingerprint erstellt und somit beispielsweise verhindert werden, dass solche Dateien das Unternehmen per E-Mail verlassen.

Fingerprints können Sie organisieren und zu einer logischen Kategorie zusammenfassen. Die Ansicht der Fingerprintkategorien ist alphabetisch sortiert.

1. Klicken Sie auf unter **Basis-Konfiguration --> Utility-Einstellungen** auf **Fingerprints**. Im rechten Fenster sehen Sie alle verfügbaren Kategorien.
2. Um eine Kategorie zu öffnen, klicken Sie eine einzelne Kategorie an. Die einzelnen Fingerprints erscheinen im rechten Fenster.
3. Die einzelnen Fingerprints können Sie vom rechten Fenster bei gedrückter Maustaste (Drag and Drop) in eine Kategorie im linken Fenster ziehen.
4. Die **Eigenschaften** der einzelnen Fingerprints im rechten Fenster öffnen Sie mit einem Doppelklick oder der rechten Maustaste.

.

Die Fingerprints aus der Kategorie **Alle Fingerprints** werden mit Drag and Drop **kopiert**. Das Ziehen aus allen anderen Kategorien hat ein **Verschieben** des Fingerprints zur Folge! Wenn Sie aus anderen Kategorien kopieren möchten, halten Sie die Strg-Taste gedrückt. Sie erkennen den Kopiervorgang an dem Plus-Zeichen.

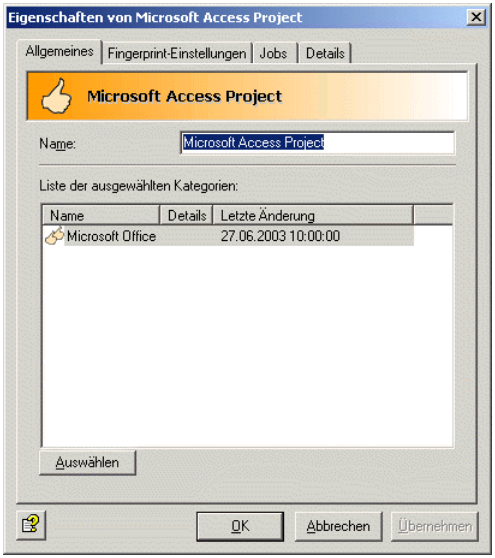
Das Löschen eines Fingerprints mit der Entf-Taste ist endgültig, egal aus welcher Kategorie! Wenn Sie einen Fingerprint nur aus einer Kategorie entfernen wollen ohne ihn wirklich zu löschen, wählen Sie mit der rechten Maustaste die Option **Entferne Fingerprint(s) aus dieser Kategorie**. Vergewissern Sie sich, dass die zu entfernenden oder zu löschenden Fingerprints in keinem iQ.Suite Job mehr verwendet werden.

Wenn Sie die Option **Prüfe Binär- und Namensmuster** aktivieren, muss sowohl das Namensmuster (Dateierweiterung) als auch das Binärmuster der geprüften Datei mit den Angaben in den Fingerprinteigenschaften übereinstimmen. Dazu müssen Sie aber auch beide Angaben gemacht haben! Wenn Sie die Option nicht aktiviert haben, aber in den Fingerprinteigenschaften beide Angaben enthalten sind, muss bei der Prüfung nur ein Merkmal zutreffen, um die Datei diesem Format zuzuordnen. Näheres über die Eingabe von Namens- und Binärmustern entnehmen Sie "Fingerprints auswählen" auf Seite 253.

Eine neue Fingerprintkategorie erstellen Sie, indem Sie im linken Fenster auf Fingerprints klicken, die rechte Maustaste drücken und **Neu --> Fingerprintkategorie** wählen. Für einen neuen Fingerprint klicken Sie mit der rechten Maustaste direkt auf die Kategorie und wählen **Neu --> Fingerprint**.

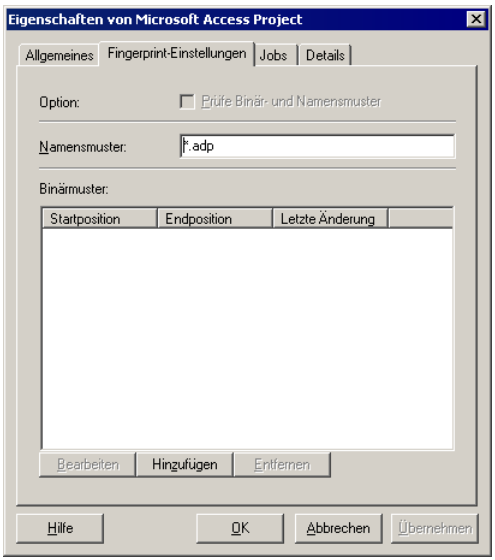
10.4.4.1 Fingerprint mit Namensmuster anlegen

Sie können eine Datei schnell durch ein Namensmuster identifizieren lassen, wenn das Binärmuster nicht bekannt ist. Wenn Sie für einen Fingerprint die Registerkarte **Allgemeines** unter **Eigenschaften** öffnen (siehe "Fingerprints konfigurieren" auf Seite 243), erhalten Sie folgendes Bild (Am Beispiel eines Microsoft-Fingerprints):



Der Fingerprint hat die Bezeichnung **Microsoft Access Project** und ist Teil der Kategorie **Microsoft Office**, die im Fenster **Kategorien** angezeigt wird. Wählen Sie die Registerkarte **Fingerprint-Einstellungen**.

Das sieht so aus:



In dem Feld **Namensmuster** geben Sie die Dateierweiterung an, welche der Dateiname besitzen muss, um auf dieses Muster zu passen.

Dabei können Sie für mehrere Zeichen mit der Wildcard * arbeiten, also beispielsweise einen Fingerprint mit dem Namensmuster *.vbs anlegen. Sie können in diesem Feld auch komplette Dateinamen angeben. Wenn Sie hier z.B. "Att01.cdf" angeben, legen Sie einen Fingerprint mit diesem Namen an und verbieten so generell Dateien mit diesem Namen, wenn Sie den Fingerprint im Job angeben.

Es sind mehrere Namensmuster pro Fingerprint möglich. Trennen Sie mehrere Muster mit einem Semikolon *(;)*

Aus der Registerkarte **Jobs** ersehen Sie, in welchen Jobs der Fingerprint verwendet wird.

Näheres zur Option **Prüfe Binär- und Namensmuster** finden Sie in “Fingerprints konfigurieren” auf Seite 243.

10.4.4.2 Binärmuster für Fingerprint anlegen

10.4.4.2.1 Formales

Binärmuster beinhalten folgende drei Informationen:

1. **Startposition**: Ab dieser Position wird innerhalb einer Datei nach einem Muster gesucht.

   Folgende Werte sind hier möglich:

"1"	Beginne beim ersten Byte der Datei
"1", "2", ...	Beginne beim erstem Byte, zweiten Byte, ... der Datei
"-1" ...	Beginne beim letzten Byte der Datei
"-6" ...	Beginne beim sechstletzten Byte der Datei

2. **Endposition**: Bis zu dieser Position wird innerhalb einer Datei nach einem Muster gesucht.

   Folgende Werte sind hier möglich:

"-1"	Suche bis zum Ende der Datei
"1","2", ... Ende	Suche bis zum 1. Byte, 2. Byte, ... der Datei
"-11" ...	Suche bis zum elftletzten Byte der Datei

3. **Hexadezimale Werte**: Dies ist das Muster, nach dem zwischen Start- und Endposition gesucht wird.
   Ein Fingerprint kann aus mehreren Binärmustern bestehen.

Rufen Sie die **Eigenschaften** eines Fingerprints auf (siehe “Fingerprints konfigurieren” auf Seite 243) und wechseln Sie zur Registerkarte **Fingerprint-Einstellungen**. Klicken Sie **Hinzufügen**.

Sie erhalten folgendes Bild:

Auf dieser Karte wird die Startposition, die Endposition und der hexadezimale Wert angegeben.

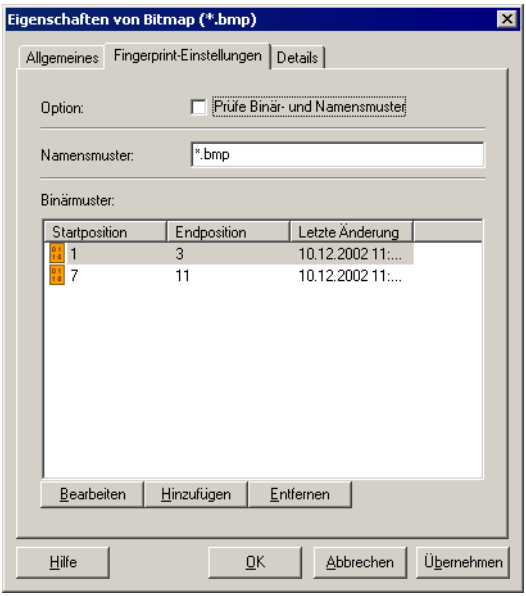
Die Startposition ist diejenige, ab welcher die angegebenen Binärdaten gesucht werden sollen. Die Position des 1. Bytes in der Datei, also der Dateianfang, ist

das Offset 1. Das 2. Byte hätte dann das Offset 2 usw. Die Endposition ist das Offset, bis zum dem das Muster gefunden werden muss.

Wenn in einem oder beiden dieser Felder der hier angegebenen Zahl ein Minuszeichen („-“) vorangestellt ist, werden die Bytes von hinten gezählt. Wenn Sie also *-1* angeben, ist das letzte Byte der Datei gemeint. *-2* wäre dann das vorletzte Byte usw. Hierbei ist es irrelevant, wie groß die Datei ist. Die Angabe Startposition *1* und Endposition *-1* bedeutet also, dass die ganze Datei nach dem angegebenen Muster durchsucht wird. Es ist möglich, zwei negative Werte anzugeben, also z.B. *-6* als Startposition und *-1* als Endposition. Damit wird zwischen dem letzten und dem sechstletzten Byte der Datei gesucht, ganz egal, wie viele Bytes die Datei letztendlich hat. Eine positive Startposition und eine negative Endposition ist immer möglich, z.B. *11* als Start- (das elfte Byte) und *-10* als Endposition (das zehntletzte Byte). Es ist nicht möglich, als Startposition einen negativen und als Endposition einen positiven Wert anzugeben.

10.4.4.2.2 Beispiel: Windows/OS2 Bitmap Dateien (*.bmp)

Wenn Sie die Fingerprint-Einstellungen einer Bitmap-Datei öffnen, erhalten Sie folgendes Bild:



Näheres zur Option **Prüfe Binär- und Namensmuster** finden Sie in "Fingerprints konfigurieren" auf Seite 243.

Öffnen Sie nun mit **Bearbeiten** den ersten Eintrag, so erhalten Sie Folgendes:

Die Startposition ist „1", die Endposition „3". Das heißt, dass zwischen dem ersten und dem dritten Byte, also zwischen dem Offset „1" und dem Offset „3" der Datei nach dem binären Muster „42 4D" gesucht wird, welches als Hexadezimale darunter eingetragen ist. Dieses Muster entspricht den Buchstaben „BM". Das ist ein Teil der Kennung einer Windows/OS2-Bitmap-Datei. Das Muster ist damit aber noch nicht komplett.

Um das Binärmuster für eine Bitmap-Datei komplett zu machen, muss ein Eintrag hinzugefügt werden. Der zweite Eintrag sieht wie folgt aus:

Hier wird zwischen dem Offset „7“ und dem Offset „11“ das Muster „00000000“ gesucht.

Erst wenn beide Binärmuster vollständig in einer Datei gefunden werden, passt die Datei auf dieses Muster und es handelt sich um eine Bitmap-Datei. Für jedes weitere in der Datei enthaltene Muster klicken Sie **Hinzufügen**.

Wenn Sie Fingerprint-Binärmuster benötigen, die nicht in der mitgelieferten Liste enthalten sind, erfragen Sie diese am besten bei dem Hersteller der Software, dessen Dateien Sie identifizieren möchten z.B. Acrobat Reader - Dateien (*.pdf) bei Adobe oder kontaktieren Sie unseren Support.

10.4.4.3 Weitere Fingerprint-Beispiele

Beispiel eines einfachen Fingerprints: ZIP Datei		
Start	Ende	HexWert
1	4	504B0304

Beispiel eines komplexeren Fingerprints: Windows Meta File		
Start	Ende	HexWert
1	13	576F72642E446F63756D656E74
1	-1	57006F007200640044006F00630075006D0065006E0074
1	10	D0CF11E0A1B11AE10000

10.4.5 Dateianhänge nach Typ verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie verschiedene Jobs für das Blocken diverser Dateiformate:

- **Blocke Archive, außer ZIP-Dateien**
  alle komprimierten Formate außer ZIP-Dateien
- **Blocke verdächtige Anhänge**
  bekannte gefährliche Anhänge wie Nimda etc.

- **Blocke Bilddateien**

  Bildformate
- **Blocke Videodateien**

  Videoformate
- **Blocke Sounddateien**

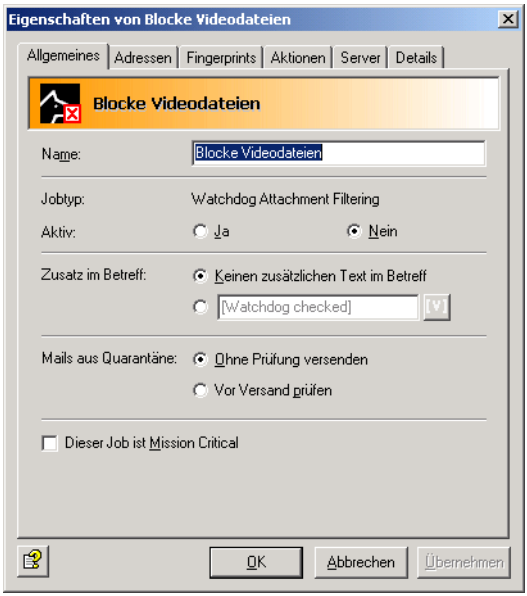
  Soundformate
- **Blocke ausführbare Dateien**

  ausführbare Dateien (**exe**, **com**, etc.)

Als Beispiel wird hier der Job **Blocke Videodateien** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

10.4.5.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Watchdog checked**. Dieser Zusatz wird, sofern aktiviert, in den Betreff jeder Mail eingefügt, die frei von verbotenen Anhängen ist.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

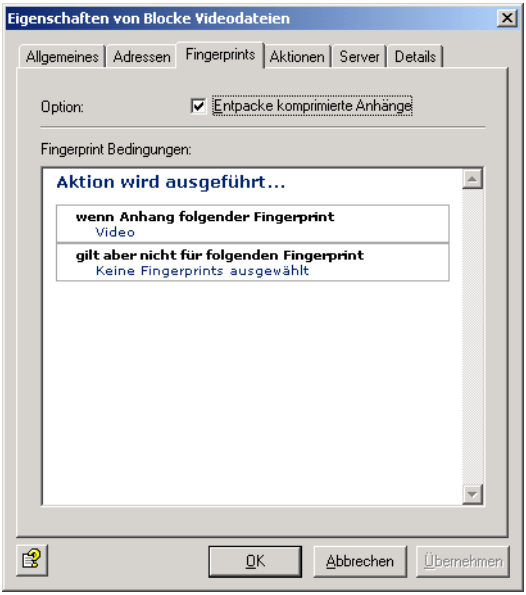
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

10.4.5.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

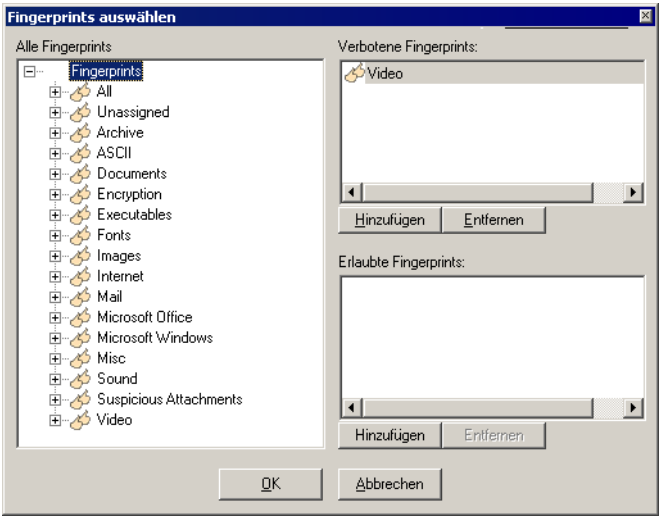
10.4.5.3 Fingerprints auswählen

Wählen Sie auf der Registerkarte **Fingerprints** die verbotenen Fingerprints aus:



Entpacke komprimierte Anhänge bedeutet, dass der interne Entpacker die Archive aufmacht und die darin liegenden Dateien auf die angegebenen Fingerprints untersucht. Ist die Checkbox nicht aktiviert, wird nur das Archiv als oberste Datei untersucht und als gepacktes Format erkannt.

Fingerprint-Bedingungen: Klicken Sie auf **Video** bzw. **keine Fingerprints ausgewählt**, um aus der Liste der Fingerprints eine Fingerprintkategorie oder einen einzelnen Fingerprint zu wählen. Sie erhalten folgende Ansicht:



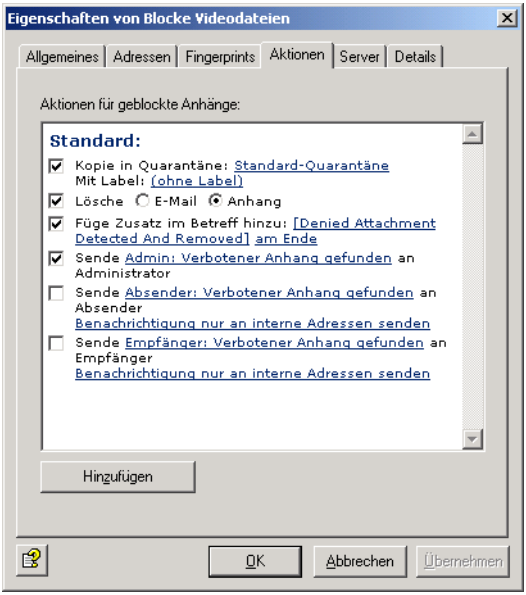
Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie der Liste der verbotenen und/oder erlaubten Fingerprints ganze Kategorien oder einzelne Fingerprints zuweisen. Öffnen Sie dafür die Kategorie im linken Fenster per Doppelklick oder mit einem Klick auf das **+**.

Sie können eine Kategorie wie z.B. Video unter **Verbotene Fingerprints** und einen einzelnen oder mehrere Fingerprint(s) dieser Kategorie unter **Erlaubte Fingerprints** als Ausnahme eintragen. Um eine bessere Übersicht zu behalten, sollten Sie nicht zu viele Kategorien von einem Job überprüfen lassen.

Näheres zu Fingerprints finden Sie unter “Fingerprints konfigurieren” auf Seite 243.

10.4.5.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job einen verbotenen Fingerprint als Anhang gefunden hat:



Eine Kopie der Mail wird in die Quarantäne gestellt und die betroffenen Anhänge werden gelöscht. Das beinhaltet, dass die Mail zwar an den Empfänger zugestellt wird, die verbotenen Anhänge aber entfernt werden. Eine Benachrichtigung über den gefundenen Fingerprint wird an Administrator versandt. Diese Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

10.4.5.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

10.4.6 E-Mail-Größe einschränken - Jobbeispiel

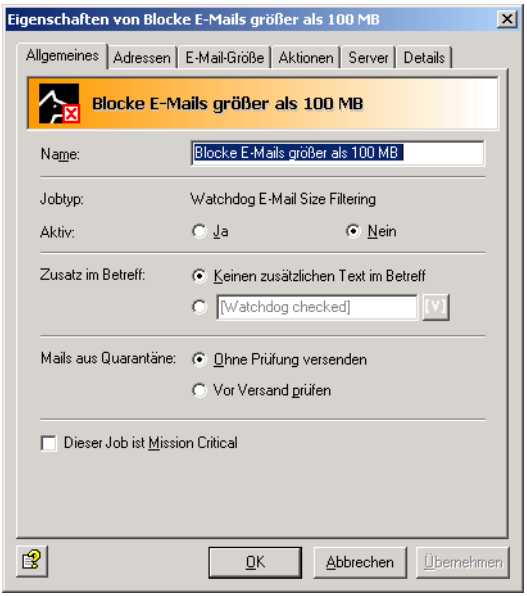
Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie den Job **Blocke E-Mails größer als 100 MB**.

Die Einschränkung der E-Mail-Größe bezieht sich auf die gesamte E-Mail inklusive Betreff, Nachrichtentext, Header und Anhang.

Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

10.4.6.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Watchdog checked**. Dieser Zusatz wird, sofern aktiviert, in den Betreff jeder Mail eingefügt, die geprüft wurde und 100 MB nicht überschreitet.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

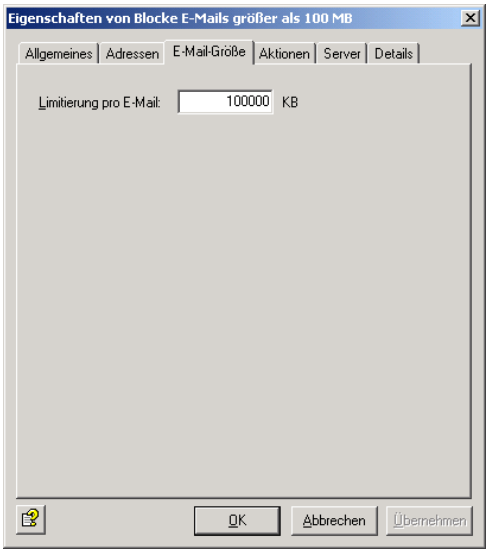
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

10.4.6.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

10.4.6.3 E-Mail-Größe festlegen

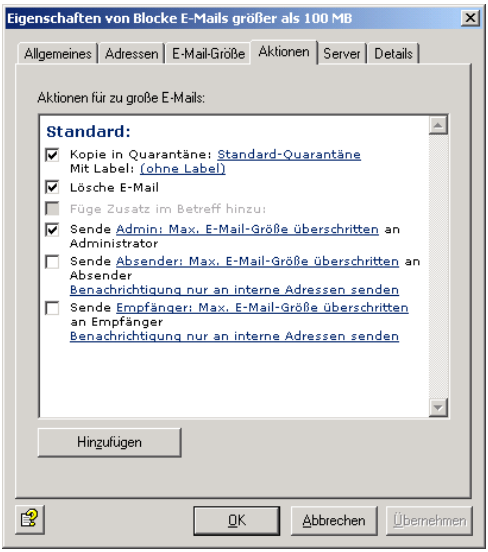
Auf der Registerkarte **E-Mail-Größe** geben Sie die gewünschte maximale E-Mail-Größe in Kilobyte an:



Jede ein- und ausgehende E-Mail darf also maximal 100.000 Kilobyte groß sein.

10.4.6.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine zu große E-Mail festgestellt hat.



Als Aktion für die E-Mail wird eine Kopie in die Quarantäne gestellt und die betroffene E-Mail gelöscht. Das beinhaltet, dass die Mail nicht an den Empfänger zugestellt wird. Eine Benachrichtigung über die zu große E-Mail wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

10.4.6.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu "Server auswählen" auf Seite 233 und "Details zum Job eingeben" auf Seite 233 durchgeführt.

10.4.7 Anhangtypen und -größe verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie verschiedene Jobs für das Blocken diverser Dateiformate und entsprechender Größen:

- **Blocke Office Dateien > 10 MB**
  Microsoft Office Dateien größer als 10 MB
- **Block Sounddateien > 5 MB**
  Sounddateien größer als 5 MB
- **Block Videodateien > 5 MB**
  Videodateien größer 5 MB

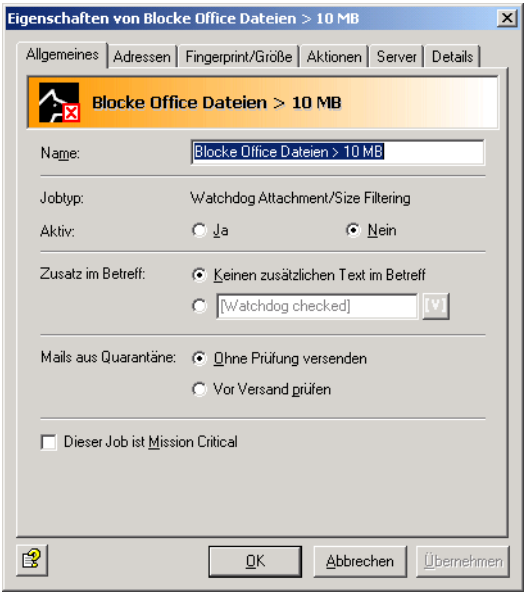
.

Die Prüfung auf Anhangformat und -größe betrifft im Gegensatz zur Prüfung der E-Mail-Größe nur die Anhänge. Betreff, Nachrichtentext und die Kopfdaten der Mail bleiben bei dieser Prüfung unberücksichtigt.

Als Beispiel wird hier der **Blocke Office Dateien > 10 MB** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

10.4.7.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Watchdog checked**.Dieser Zusatz wird, sofern aktiviert, in den Betreff jeder Mail eingefügt, die keine Microsoft Office Datei größer als 10 MB ist.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

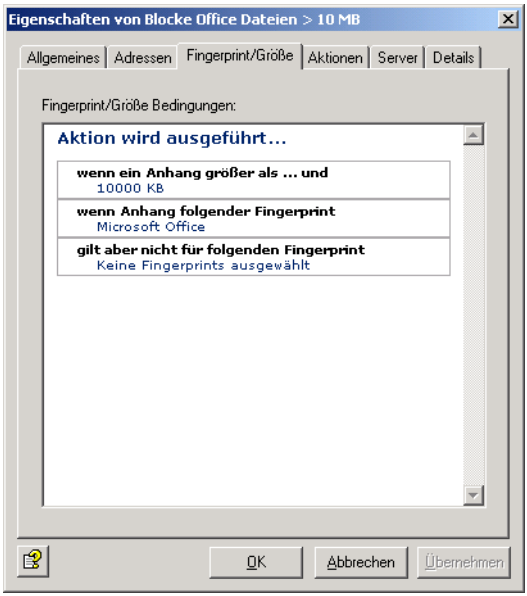
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter Dieser Job ist Mission Critical näher beschrieben.

10.4.7.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

10.4.7.3 Fingerprint/Größe bestimmen

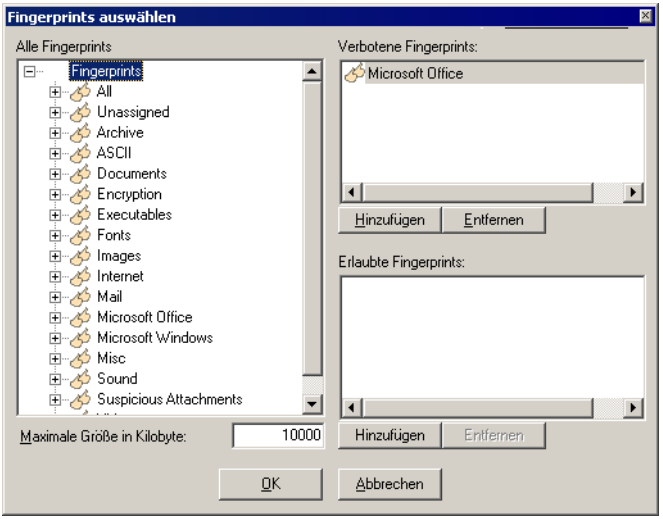
Auf der Registerkarte **Fingerprint/Größe** geben Sie die gewünschte maximale E-Mail-Größe und das Fingerprintformat an:



Im Gegensatz zur einfachen Fingerprint-Prüfung steht hier die Option **Entpacke komprimierte Anhänge** nicht zur Verfügung. Wenn Sie komprimierte Dateien in der Größe beschränken wollen, geben Sie diese Formate in diesem Job einfach an.

Fingerprint/Größe-Bedingungen: Klicken Sie auf **10.000**, um die Größe in Kilobyte festzulegen bzw. auf **Microsoft Office**, um aus der Liste der Fingerprints eine Fingerprintkategorie, einen einzelnen Fingerprint oder die maximale Größe zu wählen.

Sie erhalten folgende Ansicht:



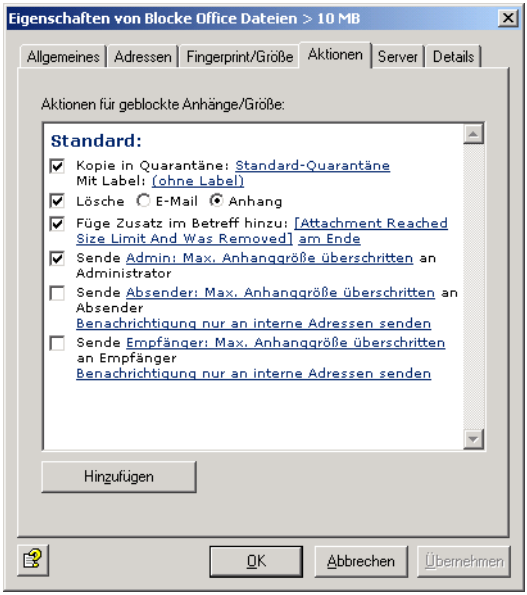
Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie der Liste der verbotenen und/oder erlaubten Fingerprints ganze Kategorien oder einzelne Fingerprints zuweisen. Öffnen Sie dafür die Kategorie im linken Fenster per Doppelklick oder mit einem Klick auf das **+**.

Sie können eine Kategorie wie z.B. Microsoft Office unter **Verbotene Fingerprints** und einen einzelnen oder mehrere Fingerprint(s) dieser Kategorie unter **Erlaubte Fingerprints** als Ausnahme eintragen. Um eine bessere Übersicht zu behalten, sollten Sie nicht zu viele Kategorien von einem Job überprüfen lassen.

Näheres über Fingerprints und über die Eingabe von Namens- und Binärmustern finden Sie unter "Fingerprints konfigurieren" auf Seite 243.

10.4.7.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine E-Mail gefunden hat, die durch einen Attachment/Size-Job verboten war.



Eine Kopie der E-Mail wird in die Quarantäne gestellt und die betroffenen Anhänge gelöscht. Die Mail wird also ohne ihren Anhang dem Empfänger zugestellt. Eine Benachrichtigung über die gefundene Einschränkung geht an den Administrator. Diese Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

10.4.7.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

11 iQ.Suite Wall

11.1 Übersicht

Mit iQ.Suite Wall prüfen Sie den Textinhalt der E-Mail oder der Anhänge, klassifizieren Mails nach Inhalten, beschränken E-Mail-Adressen im Ein-/Ausgang oder limitieren die Anzahl der Empfänger pro E-Mail.

11.1.1 Jobtypen

- die Adressprüfung

  Job: **Wall E-Mail Address Filtering**
- die Inhaltsprüfung

  Job: **Wall Content Filtering**
- die Anti-Spam-Prüfung

  Job: **Wall Spam Filtering**
- die Anti-Spam-Prüfung über DCC-Server

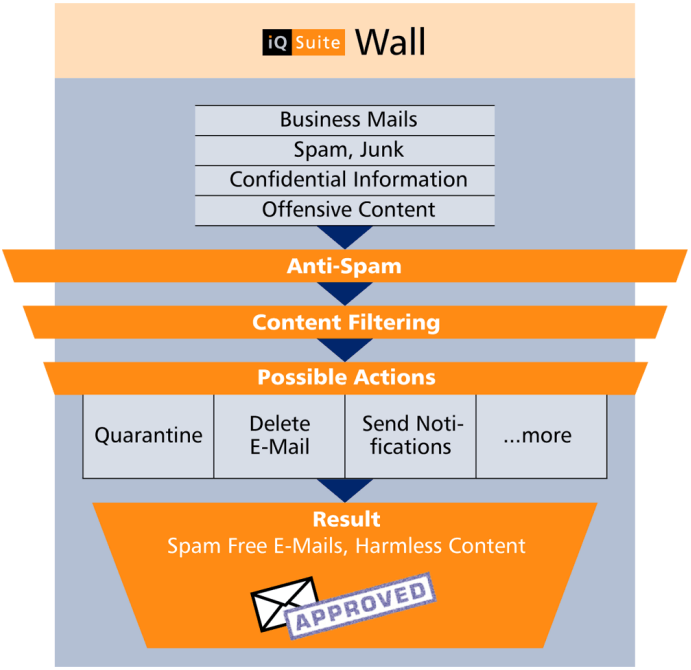
  Job: **Wall DCC Spam Filtering**
- die Textklassifikation mit CORE

  Job: **Wall CORE Classification**
- Prüfung auf Anzahl der Empfänger

  Job: **Wall Recipient Limit Filtering**

Legen Sie für jeden Einschränkungstyp einen separaten Job an! Die Jobtypen lassen sich später nicht mehr ändern.

Die genaue Vorgehensweise für die Job-Einrichtung entnehmen Sie bitte den Jobbeispiel-Beschreibungen, z.B. “Absender und/oder Empfänger verbieten - Jobbeispiel” auf Seite 268. Grafisch dargestellt sieht die Arbeitsweise wie folgt aus:



11.2 Adressprüfung

Die Adressprüfung konzentriert sich auf die Absender und die Empfänger einer E-Mail. Dabei können Sie bestimmte Absender verbieten, so dass keine Mail mehr von diesen zu Ihren Benutzern gelangt oder aber auch bestimmte Empfänger, so dass keiner Ihrer Mitarbeiter (oder nur ausgewählte) an gewisse Empfänger E-Mails versenden können.

Bei der Adressprüfung können folgende Objekte verwendet werden:

- Mail-Enabled Active Directory Benutzer
- Mail-Enabled Active Directory Gruppen
- Mail-Enabled Active Directory Kontakte
- Frei definierbare SMTP Adressen inkl. Wildcards
- [INTERN] = Als in der iQ.Suite definierten internen Domänen
- [EXTERN] = Alle Adressen, die nicht [INTERN] sind
- "Administrator" = Die in der iQ.Suite als Administrator definierten E-Mail-Adressen.

Maßgebend für die Definition, ob es sich um einen Absender oder einen Empfänger handelt, ist immer der Eintrag in den entsprechenden Feldern der E-Mail. Ein Absender kann also sowohl ein Mitarbeiter Ihres Unternehmens sein, der eine E-Mail nach außen sendet, als auch eine externe Person, die einem Mitarbeiter Ihres Unternehmens eine E-Mail schickt. Sie können sowohl Absender als auch Empfänger als Person oder als Gruppe definieren.

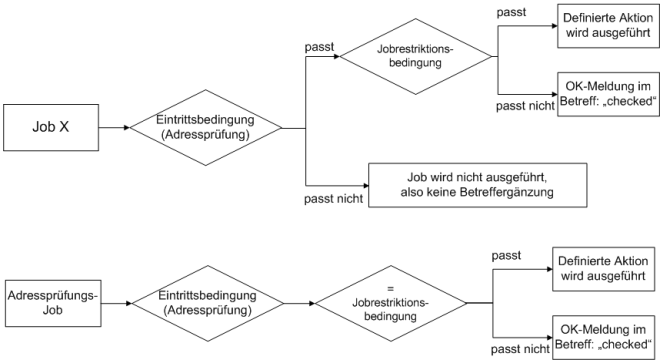
Bei der Adressprüfung sind generell folgende Wildcards möglich:

- Stern (*)
  Der Stern symbolisiert den Platzhalter für ein **oder** mehrere beliebige Buchstaben und/oder Zahlen. Der Stern kann mehrfach mitten im Begriff eingesetzt werden.
- Fragezeichen (?)
  Das Fragezeichen dagegen ist der Platzhalter für ein einziges Zeichen. Auch das Fragezeichen kann mehrfach mitten im Begriff vorkommen.

Beispiel: Wenn Sie einen verbotenen Absender angeben, können Sie statt einzelner E-Mail-Adressen auch tom*@*.* nehmen. Das heißt, dass alle E-Mails, die von einem Tom mit beliebiger Erweiterung (also auch Nachnamen) von welcher Domäne auch immer gesendet werden, als Absender verboten sind. Darunter fällt dann auch Ihr eigener Mitarbeiter namens Tom Jones, der somit unter die Einschränkung und dessen E-Mails unter die definierten Aktionen fallen. Eine bestimmte Domäne können Sie zum Beispiel als *@domain.com definieren. Damit gelten alle Absender bzw. Empfänger dieser Domäne als verboten. Einen Job zur Adressprüfung mit dem Verbot einer ganzen Domäne sollten Sie nur mit großer Vorsicht serverübergreifend für alle anlegen. Es ist nicht immer klar, welche Adressen privater und welche beruflicher Natur sind. Bedenken Sie, dass kleinere Geschäftspartner durchaus E-Mail-Adressen unter der Domäne @t-online.de oder @aol.com besitzen.

Die Adressprüfung ist ein einfaches Mittel, bekannte Spamadressen auszufiltern. Die „üblichen Verdächtigen" können vom Job auf dem Server abgefangen und sofort gelöscht werden.

Da bei den Adressprüfungsjobs die Eintrittsbedingung mit der Jobrestriktionsbedingung übereinstimmt, wird ein ggf. konfigurierter **Zusatz im Betreff** im OK-Fall - im Gegensatz zu den anderen Jobtypen - auch angefügt, wenn die Eintrittsbedingung nicht zutreffend ist:



Folgende Aktionen sind möglich:

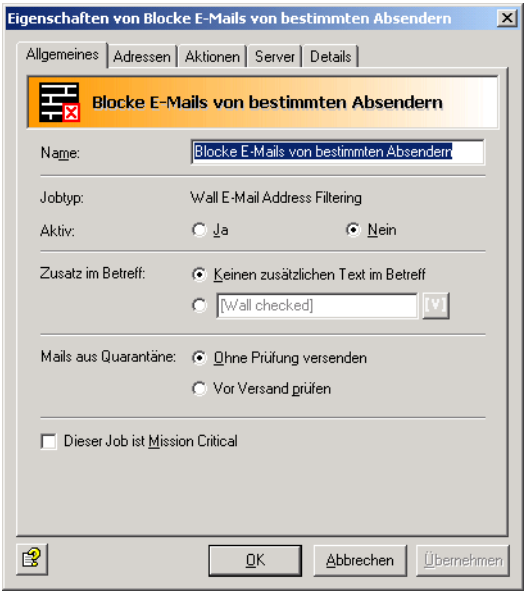
- Zusatz im Betreff
- Gesamte Mail in Quarantäne kopieren
- Betroffene E-Mail löschen und nicht zustellen
- Ausführen einer externen Anwendung
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- X-Header-Feld hinzufügen
- Mail umleiten

11.2.1 Absender und/oder Empfänger verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie einen vorkonfigurierten Job für die Adressprüfung. Öffnen Sie den Job **Blocke E-Mails von bestimmten Absendern** mit einem Doppelklick.

11.2.1.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Wall checked**. Dieser Zusatz wird, sofern aktiviert, in den Betreff jeder Mail eingefügt, deren Absender erlaubt sind.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

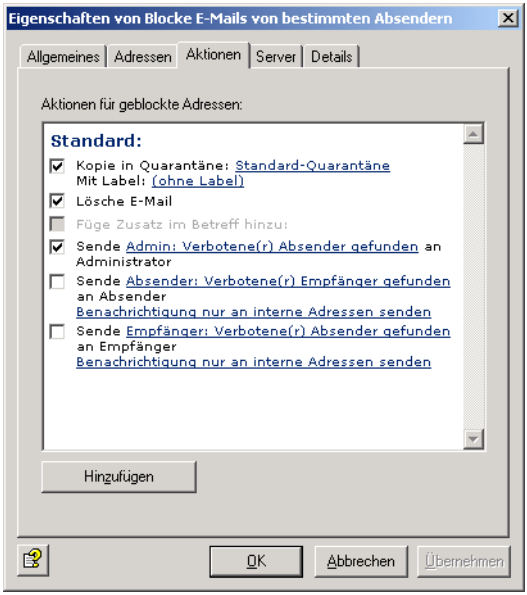
Näheres zum erneuten Versand aus der Quarantäne finden Sie in "Aus Quarantäne senden" auf Seite 130. Die Option **Mission Critical** finden Sie unter **Dieser Job ist Mission Critical** näher beschrieben.

11.2.1.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

11.2.1.3 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine E-Mail mit verbotenen Absendern gefunden hat.



Als Aktion wird eine Kopie in die Quarantäne gestellt und die betroffene E-Mail gelöscht. Das beinhaltet, dass die Mail dem Empfänger **nicht** zugestellt wird. Eine Benachrichtigung über die Verletzung der Adress-Richtlinien wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[27].

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

11.2.1.4 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

11.3 Inhaltsprüfung mit Wortlisten

iQ.Suite Wall verwendet vordefinierte Wortlisten, um nach unerwünschten Textinhalten zu suchen.

Dabei können folgende Bestandteile der E-Mail geprüft werden:

- Betreff
- Nachrichtentext
- Anhänge

Die Inhaltssuche kann auf bestimmte Absender bzw. Empfänger eingeschränkt werden. Damit können z.B. nur von außen eintreffende Mails auf Pornographie, Rassismus etc. untersucht werden. Bei Mails von internen Absendern nach außen könnten Sie hingegen die Mails nach Firmeninterna durchsuchen lassen. Die Mails werden anhand der zu verwendenden Wortlisten durchsucht und die von Ihnen angegebenen Wörter oder Sätze innerhalb der Wortlisten gelten ab einem bestimmten Schwellwert als verboten, sobald diese Wortliste im Job aktiviert ist. Auch die Zeichenumsetzung wird im Job festgelegt. Bei erreichtem Schwellwert setzt der Job die Aktionen in Gang, die Sie vorher in der Registerkarte **Aktionen** festgelegt haben.

Hier ein Beispiel für die Arbeitsweise eines Jobs für die Inhaltsprüfung. Der Job prüft eine E-Mail mit dem Ergebnis: Verbotener Inhalt gefunden. Daraufhin wird ein Alarm ausgelöst und eine Reihe von Aktionen in Gang gesetzt, die Sie selbst im Job unter Aktionen definieren können. Wir nehmen an, dass Sie Folgendes festgelegt haben:

---

27. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100

1. Die Mail wird in den von Ihnen gewählten Ordner (Quarantäne) verschoben und dem Empfänger nicht zugestellt.
2. Es werden Nachrichten an Administrator, Absender und Empfänger erstellt, die mit den relevanten Informationen des Wall-Jobs versehen sind.

Die möglichen Aktionen sind die gleichen wie bei der Adressprüfung.

11.3.1 Wortlisten einrichten

1. Klicken Sie auf **Wortlisten**.
2. Öffnen Sie mit einem Doppelklick eine Wortliste im rechten Fenster.
3. Vergeben Sie auf der Registerkarte **Allgemeines** einen Namen für die Wortliste.
4. Geben Sie der Wortliste eine **Wertigkeit** von 1 bis 200. Diese Wertigkeit gilt pro Wort oder Phrase und bestimmt sowohl das Verhältnis zu anderen Wortlisten als auch, wie stark die Wortliste im Job berücksichtigt wird. Näheres zu Wertigkeiten finden Sie in “Inhaltsprüfung mit Wortlisten” auf Seite 271 und “Textinhalte prüfen und verbieten - Jobbeispiel” auf Seite 275.
5. Klicken Sie in das Eingabefeld für die Worte und fügen Sie die Wörter/Phrasen hinzu, die Sie verbieten wollen. Die einzelnen Wörter/Phrasen werden mit einem Absatz (Enter-Taste) voneinander getrennt.
   Folgende Wildcards sind in Wortlisten möglich:
   - Stern (*)

     Der Stern bedeutet, dass das gesuchte Wort/Phrase auch ein Teil größeren Wortes sein **kann**, aber nicht muss. Beispiel: **check** findet das einzelne Wort „check“ genauso wie das Wort „checkpoint“, „intercheck“ oder „intercheckpoint“. *check** findet „check“ genauso wie „checkpoint“. Der Stern muss entweder am Anfang eines Wortes/Phrase oder am Ende eingesetzt werden.

   - Pluszeichen (+)

     Das Pluszeichen bedeutet das Gleiche wie der Stern mit dem Unterschied, dass das gesuchte Wort ein Teil eines größeren Wortes sein **muss**. Beispiel: *+check+* findet nur „checkpoint“, „intercheck“ oder „intercheckpoint“, aber nicht „check“. *check+* findet aber nur „check-

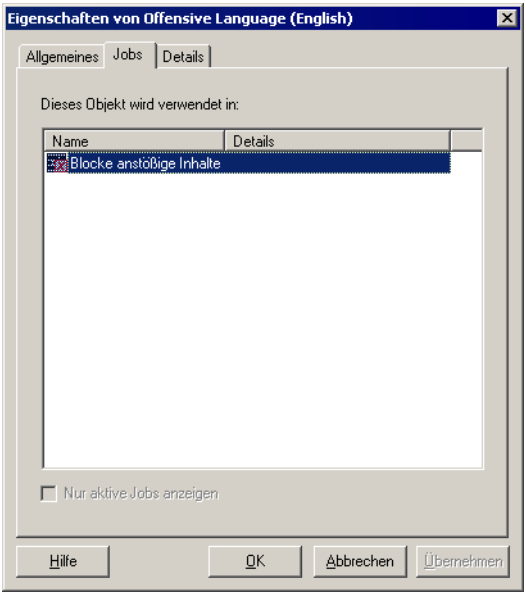
point“. Das Pluszeichen muss ebenfalls am Anfang oder am Ende eines Wortes/Phrase eingesetzt werden.

Wenn Sie weder einen Stern noch ein Pluszeichen in Ihren Wörtern/Phrasen der Wortliste einsetzen, so muss genau dieses eingegebene Wort exakt gefunden werden. Also: Wenn Sie *check* eingeben, so wird auch nur das einzelne Wort „check“ gefunden.

6. Sortieren Sie die Wortliste nach Wunsch aufsteigend oder absteigend, indem Sie auf für aufsteigend und für absteigend klicken.

Eine neue Wortliste erstellen Sie, indem Sie mit der rechten Maustaste auf **Wortlisten** klicken und **Neu --> Wortliste** wählen.

In welche Jobs ein Objekt eingebunden ist, ersehen Sie aus der Registerkarte **Jobs**:

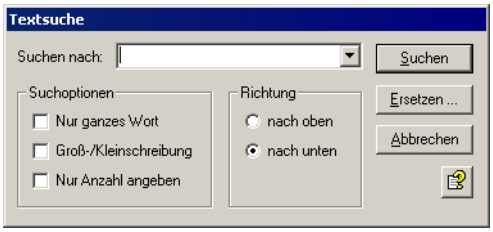


.

Um die Wortlisten im Job einzusetzen, wählen Sie in der Richtlinien-Konfiguration einen Content-Filtering Job aus, aktivieren die entsprechende Wortliste und bestimmen einen Gesamt-Schwellwert (von 1 bis 10.000). Sobald dieser Schwellwert durch das Addieren aller Wertigkeiten (gefundene Wörter) der aktiven Wortlisten erreicht wurde, treten die definierten Aktionen in Kraft. Nähere Informationen erhalten Sie unter "Textinhalte prüfen und verbieten - Jobbeispiel" auf Seite 275.

11.3.1.1 Textsuche in Wortlisten

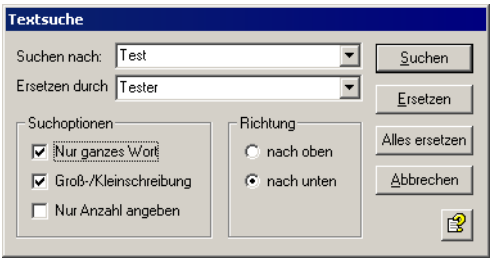
Sie können in Wortlisten nach Begriffen suchen und sie ggf. ersetzen. Öffnen Sie die Wortliste mit einem Doppelklick und klicken Sie auf das Symbol für Textsuche:



Wenn Sie keine Zusatzoption angeben, so wird die Zeichenfolge überall gefunden, also auch in Teilen eines Wortes oder einer Phrase.

- **Nur ganzes Wort**:
  Als Trennzeichen zwischen Wörtern gelten alle nicht-alphanumerischen Zeichen inklusive eines Absatz- bzw. Zeilenwechsels.
- **Groß-/Kleinschreibung**:
  Berücksichtigt die Groß- und Kleinschreibung bei der Suche.
- **Nur Anzahl angeben**:
  Die Treffer werden nicht direkt angesprungen, sondern durchgezählt und das Ergebnis in Form einer Mitteilung ausgegeben:

Klicken Sie auf die Schaltfläche **Ersetzen**, wenn Sie einen bestimmten Begriff durch einen anderen ersetzen möchten:



Die Textsuche können Sie auch für das Suchen und Ersetzen in eigenen Adressen verwenden. Siehe dazu “Adresslisten” auf Seite 90.

11.3.2 Textinhalte prüfen und verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration --> Jobbeispiele** finden Sie verschiedene Jobs für die Inhaltsprüfung mit Wortlisten:

- **Blocke anstößige Inhalte**

  Suchen nach ordinärer und pornografischer Sprache
- **Blocke Scriptkommandos**

  Suchen nach Script-Befehlen, die Schaden anrichten können
- **Blocke E-Mails mit Lebensläufen**

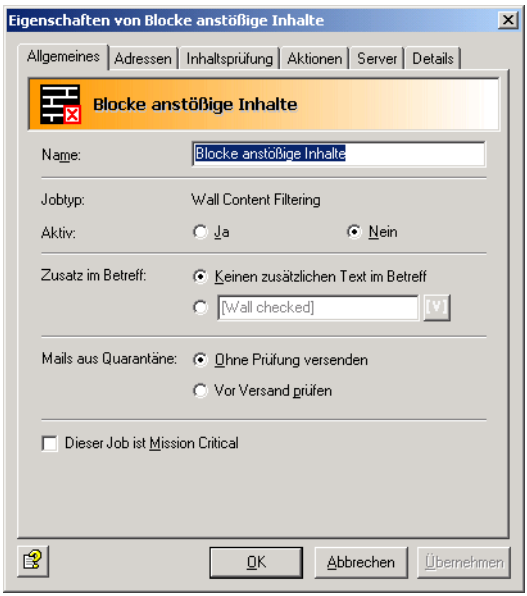
  Suchen nach Begriffen aus Lebensläufen
- **Blocke E-Mails von „Nigeria-Connection“**

  Suchen nach speziellen Begriffen in den „Nigeria“-E-Mails

Als Beispiel wird hier **Blocke anstößige Inhalte** behandelt. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

11.3.2.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Wall checked**. Dieser Zusatz wird, sofern aktiviert, in den Betreff jeder Mail eingefügt, welche die Inhaltsprüfung bestanden hat.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

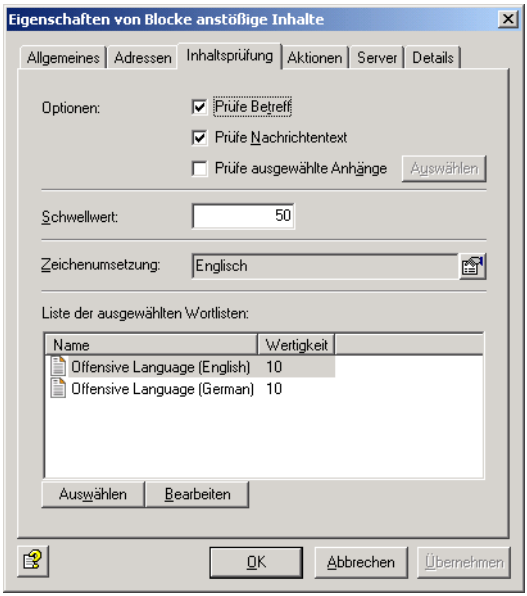
Näheres zum erneuten Versand aus der Quarantäne finden Sie in "Aus Quarantäne senden" auf Seite 130. Die Option **Mission Critical** finden Sie unter **Dieser Job ist Mission Critical** näher beschrieben.

11.3.2.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in "Adresslisten" auf Seite 90.

11.3.2.3 Wortlisten auswählen

In der Registerkarte **Inhaltsprüfung** stellen Sie ein, welche Wortlisten mit diesem Job aufgerufen werden sollen.



Dieser Job prüft den Betreff. Der Gesamt-Schwellwert ist auf 50 festgelegt. Damit wird bei 5 gefundenen Wörtern/Phrasen aus der Wortliste **Offensive Language (English)** oder **Offensive Language (German)** die definierten Aktionen ausgeführt. Die Rechnung:

Jedes Wort oder jede Phrase der Liste **Offensive Language** ist mit der Wertigkeit 10 belegt. Damit werden bei mindestens 5 gefundenen Wörtern/Phrasen aus diesen Listen die Aktionen ausgeführt. Erklärung:

Jedes Wort oder jede Phrase der Liste **Offensive Language** ist mit der Wertigkeit 1 belegt. Jedes gefundene Wort/Phrase aus dieser Liste wird gezählt, mit der Wertigkeit multipliziert, danach alle multiplizierten Werte addiert und mit dem Schwellwert verglichen. In diesem Fall also:

5 Wörter, die auf der Liste stehen, wurden in der E-Mail gefunden. Jedes davon wird mit der Wertigkeit (10) multipliziert: 1 x 10 = 10. Dieser Wert wird fünfmal addiert: 10 + 10 + 10 + 10 + 10 = 50. Verglichen mit dem Schwellwert 50 = Aktion wird ausgelöst.

Werden in diesem Fall nur 4 Wörter in der E-Mail entdeckt, beträgt der Gesamtwert nur 40, der Schwellwert ist nicht erreicht und es wird keine Aktion in Gang gesetzt.

Ein anderes Beispiel:

Sie prüfen mit zwei verschiedenen Wortlisten den Betreff und den Nachrichtentext einer E-Mail auf verbotenen Inhalt.

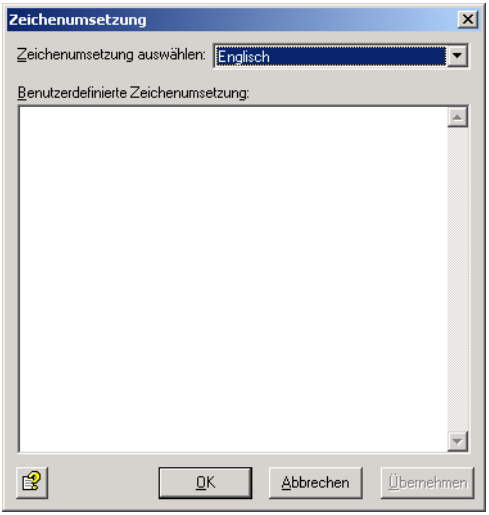
Der Gesamt-Schwellwert ist im Job auf 20 festgelegt und die erste im Job angegebene Wortliste hat eine Wertigkeit von 20. Die zweite in diesem Job angegebene Wortliste hat eine Wertigkeit von 1. Damit wird bei 1 gefundenen Wort/Phrase aus der ersten Wortliste oder alternativ bei 20 gefundenen Begriffen aus der zweiten Wortliste die definierten Aktionen ausgeführt. Die Rechnung:

Jedes Wort oder jede Phrase der ersten Wortliste ist mit der Wertigkeit 20 belegt. Damit ist bei einer einzigen gefundenen Phrase aus dieser Liste der Schwellwert bereits erreicht und die Aktion wird durchgeführt.

Jedes Wort oder jede Phrase der zweite Wortliste ist mit der Wertigkeit 1 belegt. Jedes gefundene Wort/Phrase aus dieser Liste wird gezählt, mit der Wertigkeit multipliziert, danach alle multiplizierten Werte addiert und mit dem Schwellwert verglichen. Wenn hier also 21 Wörter, die auf der Liste stehen, in der E-Mail gefunden werden, wird jedes davon mit der Wertigkeit (1) multipliziert: 1 x 1 = 1.

Dieser Wert wird 21 mal addiert, also 21 mal 1 = 21. Verglichen mit dem Schwellwert 20 = Aktion wird ausgelöst.

Um die Wörter in den Wortlisten korrekt mit allen Sonderzeichen einer Sprache erkennen zu können, wählen Sie mit der Auswahlschaltfläche die **Zeichenumsetzung** aus. Sie erhalten folgenden Dialog:

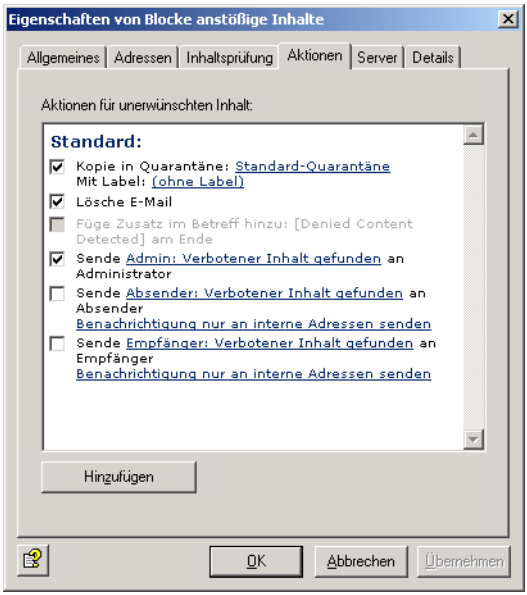


Zur Wahl stehen Ihnen im Pull-Down-Menü die Sprachen **Englisch** und **Deutsch** und die **Benutzerdefinierte Zeichenumsetzung**. Bei der Auswahl der deutschen Zeichenumsetzung können Sie Ihre Wortlisten mit deutschen Umlauten (ö, ä, ...) anlegen, da diese automatisch erkannt werden. Sonderzeichen aus anderen Sprachen wie z.B. französische Accents erfordern eine benutzerdefinierte Zeichenumsetzung.

Wenn Sie Inhalte aus verschiedenen Sprachen erkennen wollen, legen Sie die entsprechenden Wortlisten an und richten Sie pro Sprache einen Job ein. Definieren Sie bei Sprachen wie Französisch und Spanisch eine benutzerdefinierte Zeichenumsetzung. **Bitte wenden Sie sich für diese Konfiguration an unseren Support**.

11.3.2.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine E-Mail mit verbotenem Inhalt gefunden hat.



Als Aktion wird eine Kopie in die Quarantäne gestellt und die betroffene E-Mail gelöscht. Das beinhaltet, dass die Mail dem Empfänger **nicht** zugestellt wird. Eine Benachrichtigung über die Verletzung der Unternehmens-Richtlinien wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell über die HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden[28].

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

28. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100

11.3.2.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu "Server auswählen" auf Seite 233 und "Details zum Job eingeben" auf Seite 233 durchgeführt.

11.4 Anti-Spam mit dem Wall Spam Filtering Job

Die Anti-Spam Prüfung sucht in E-Mails speziell nach Merkmalen, die auf Spam hinweisen. Nun ist Spam, im Gegensatz zu Viren, nicht immer eindeutig als solcher erkennbar. Spammer versenden ganz unterschiedliche Inhalte in den unterschiedlichsten Formen, immer darauf bedacht, ihre Mails nicht als das erkennen zu lassen, was sie sind: Nämlich Spam. Dazu benutzen Spammer immer neue Tricks, um an der Erkennung durch Spam-Filter vorbei zu kommen. So muss auch ein Anti-Spam-Job berücksichtigen, dass eine Mail mitunter nicht eindeutig als Spam identifizierbar sein kann. Daher arbeitet der Spam-Filtering Job mit den unterschiedlichsten Spam-Kriterien, die in **definitive** und **kombinierte Kriterien** aufgeteilt sind. Der Job untersucht die Mail anhand der definitiven Kriterien auf absolut eindeutige Spam-Merkmale und urteilt nach der Prüfung: 100% Spam oder 100% Nicht-Spam. Anhand der kombinierten Kriterien wird die „Grauzone" untersucht, um zu errechnen, mit welcher Wahrscheinlichkeit die geprüfte E-Mail Spam ist (= **Spam-Wahrscheinlichkeit**). Dabei ist die Spam-Wahrscheinlichkeit der definitiven Kriterien immer 0% oder 100%, die der kombinierten Kriterien kann von 1 bis 99 reichen.

Einen vorkonfigurierten **Wall Spam Filtering** Job finden Sie in der **Richtlinien-Konfiguration**. Der Job enthält eine Reihe von Analysen und prüft folgende Bestandteile der E-Mail:

- E-Mail-Kopfzeilen (Header)
- Betreff
- Nachrichtentext

Auch hier werden - wie in der normalen Inhaltsprüfung - vordefinierte Wortlisten unterschiedlichsten Inhalts verwendet, um nach Spam-Textinhalten zu suchen.

In der „Grauzone" treten einige der kombinierten Kriterien bei Spam-Mails gehäuft auf und andere Kriterien sind eher ein Hinweis für Nicht-Spam-Mails.

Jedes kombinierte Kriterium für sich allein ist normalerweise nur ein Hinweis darauf, ob eine Mail bestimmte Merkmale aufweist, die auf Spam hindeuten. Je mehr Kriterien einen hohen Wert für Spam in einer Mail ausweisen, desto sicherer kann man davon ausgehen, dass es sich in der Tat um eine Spam-Mail handelt. Durch die Kombination der Einzelergebnisse dieser Kriterien (daher: kombinierte Kriterien) ergibt sich im Job eine Maßzahl, die den Grad der Überzeugung ausdrückt, dass es sich bei dieser Mail um Spam handelt (= Spam-Wahrscheinlichkeit).

Der vorkonfigurierte Job ist so eingestellt, dass eine E-Mail eine hohe **Spam-Wahrscheinlichkeit** von z.B. über 91% nur erreichen kann, wenn für mehrere kombinierte Kriterien deutliche Hinweise auf Spam gefunden wird.

Im Job werden bis zu vier Bereiche dieser Spam-Wahrscheinlichkeit unterschieden. Sie können die Grenzen zwischen vier Bereichen (Spam-Wahrscheinlichkeit = Schwellwerte) per Schieberegler selbst festlegen und für jeden festgelegten Bereich die Aktionen definieren, die der Job mit den E-Mails ausführen soll, deren Spam-Wahrscheinlichkeit im entsprechenden Bereich liegt. So könnten Sie z.B. konfigurieren, dass

- definitiver „Nicht-Spam“ mit einer **Spam-Wahrscheinlichkeit** von 0% normal zugestellt wird,
- unter einer Spam-Wahrscheinlichkeit von 10% die E-Mail ebenfalls normal zugestellt wird. Eine Option könnte sein, diese Mails für die Klassifizierung mit CORE in die Quarantäne **Anti-Spam: Low** zu stellen (siehe auch “CORE Klassifikation” auf Seite 312),
- zwischen 10% und 50% Spam-Wahrscheinlichkeit das **SCL-Feld** in Exchange 2003 ausgewertet wird[29], so dass die Mail automatisch in den Junk-Mail-Ordner des Empfängers verschoben wird oder die Mails in die Quarantäne **Anti-Spam: Medium** zu stellen,
  - so dass der Administrator sie für CORE klassifizieren kann und

29. siehe dazu auch “Schreibe Spam-Ergebnis in Exchange SCL Feld” auf Seite 293

- die Empfänger eine Sammelbenachrichtigung über die quarantänierten Mails erhalten und sie ggf. anfordern können,

- Mails über 50% Spam-Wahrscheinlichkeit gleich gelöscht werden. Auch hier können Sie die Mails für die Klassifizierung mit CORE in die Quarantäne **Anti-Spam: High** stellen.

Folgende Aktionen sind möglich:

- Zusatz im Betreff
- Gesamte Mail in Quarantäne kopieren
- Betroffene E-Mail löschen und nicht zustellen
- Ausführen einer externen Anwendung
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- X-Header-Feld hinzufügen
- Mail umleiten

Die einzelnen Schwellwertbereiche:

1. **Spam-Wahrscheinlichkeit: Keine**. Vorkonfiguriert: 0.
2. **Spam-Wahrscheinlichkeit: Niedrig**. Vorkonfiguriert: 0 - 9.
3. **Spam-Wahrscheinlichkeit: Mittel**. Vorkonfiguriert: 10 - 49.
4. **Spam-Wahrscheinlichkeit: Hoch**. Vorkonfiguriert: 50 -100.

Die Bereiche **Niedrig**, **Mittel** und **Hoch** können per Regler definiert und dazugehörige Aktionen eingerichtet werden. Je nachdem, in welchen Bereich die E-Mail nach der Prüfung einsortiert wurde, wird die für diesen Schwellwertbereich definierte Aktion ausgelöst. Für die Spam-Wahrscheinlichkeit **Keine** können Sie einen **Zusatz im Betreff** konfigurieren.

Wichtig für eine gute Anti-Spam-Lösung ist auch die effektive Vermeidung von falsch klassifizierten Mails (False Positives) und die effiziente Verwendung der für die Spam-Prüfung zur Verfügung stehenden Rechenleistung im Produktivbetrieb. Die definitiven Ausschlusskriterien (**= Definitive Kriterien**) sind daher den kombinierten Kriterien so vorgeschaltet, dass bei deren Eintreten die weitere Untersu-

chung der Mail auf Spam-Merkmale unterbleiben kann. Die Ausschlusskriterien dienen dazu, die durchzuführenden Spam-Untersuchungen auf solche Mails zu beschränken, für die nicht bereits z.B. aufgrund des Absenders ausgeschlossen werden kann, dass es sich um Spam handelt.

Bei Zutreffen eines definitiven Kriteriums beträgt die Spam-Wahrscheinlichkeit immer 0% oder 100% und fällt damit in den Wahrscheinlichkeitsbereich **Keine** oder **Hoch** mit den entsprechenden Aktionen.

Selbstverständlich beeinflussen diese Kriterien nicht die Prüfung durch die anderen konfigurierten und aktiven Jobs wie z.B. die Prüfung auf Dateianhänge durch iQ.Suite Watchdog. Wenn Sie also das definitive „Kein-Spam“-Kriterium **E-Mails mit Anhängen** aktiviert und den Schwellwert (**Minimum-Anzahl**) auf 2 eingestellt haben, bedeutet das nur, dass der Spam-Filtering Job diese Mails sofort in den Spam-Wahrscheinlichkeitsbereich **Keine** einsortiert und nicht, dass ein Watchdog Job diese 2 Anhänge plötzlich völlig ungeprüft in Ihr Netzwerk gelangen lässt.

.

Normalerweise ist es nicht nötig, die kombinierten Kriterien anzupassen. Versuchen Sie bei nicht zufrieden stellenden Spam-Erkennungsraten, zunächst die definitiven Spam-Kriterien (Ausschlusskriterien) zu optimieren (siehe unten). Trainieren Sie ggf. Ihren eigenen CORE Spam-Klassifikator (siehe “CORE Klassifikation” auf Seite 312).

Im Job können die folgenden Ausschlusskriterien konfiguriert werden:

11.4.1 Definitive Kein-Spam-Kriterien

Kriterium	Beschreibung
E-Mails der folgenden Absender (Whitelist)	Whitelist: Adressen aller bekannten Absender, die immer erlaubt sind und die eindeutig keinen Spam versenden. Dies sind im Prinzip alle regelmäßigen Kommunikationspartner und die Domänen von Kunden und Lieferanten. Je vollständiger diese Liste gehalten wird, desto weniger wird Ihr System mit unnötigen Prüfungen belastet.
E-Mails von Active Directory Benutzern	Weitere vertrauenswürdigen Adressen sind alle im Active Directory eingetragenen Benutzer und Kontakte.
Wörter im Betreff	Alle E-Mails mit bestimmten Wörtern im Betreff werden ohne Prüfung auf Spam durchgelassen. Mit dieser Funktion ist es möglich, bestimmte „Passwörter“ zu vereinbaren, so dass Mails kritischen Inhalts trotzdem ohne Spam-Prüfung zugestellt werden können. Diese Wörter werden über eine Wortliste definiert und die Wortliste im Anti-Spam-Job angegeben. Mit der Zusatzoption kann neben dem Betreff auch der Nachrichtentext auf diese Wörter geprüft werden.
E-Mails mit Anhängen	E-Mails mit Dateianhängen. Spams werden praktisch immer ohne Anhänge versendet. Außerdem kann hier ein Schwellwert eingetragen werden. Beispiel: Minimum-Anzahl = 2 bedeutet, dass alle Mails mit zwei oder mehr Dateianhängen ohne Spam-Prüfung zugestellt werden.
E-Mails mit Mindestgröße von	Spam-Mails sind in der Regel klein. Deshalb sind große E-Mails meist kein Spam. Hier kann ein Schwellwert eingestellt werden, ab dem die E-Mails nicht mehr durch die Spam-Prüfung laufen.
E-Mails sind in TNEF-Format	TNEF Mails. Dieses Exchange-spezifische Format wird bisher nicht von Spammern benutzt.

11.4.1 Definitive Kein-Spam-Kriterien

Kriterium	Beschreibung
E-Mails sind verschlüsselt oder signiert	Verschlüsselte und/oder signierte Mails. Spammer versenden bisher keine verschlüsselten oder signierten E-Mails.
Microsoft Exchange „Kein Spam“ SCL-Wert Siehe auch Schreibe Spam-Ergebnis in Exchange SCL Feld.	Spam Confidence Level (SCL), Spam-Filter (Intelligent Message Filter (IMF)) ab Exchange 2003. SCL kann ganzzahlige Werte zwischen -1 und 9 annehmen. -1 wird von Exchange für Mails von Absendern aus der gleichen Exchange-Organisation vergeben. Dieser Wert wird vom Wall Spam Filtering Job als definitives „Kein Spam“-Kriterium gewertet.

11.4.2 Definitive Spam-Kriterien

Kriterium	Beschreibung
E-Mails der folgenden Absender (Blacklist)	Blacklist: Adressen aller Absender, die immer als Spam-Absender identifiziert werden. Die Standardkonfiguration enthält bereits eine Liste von bekannten Adressen. Sie können eigene zusätzliche Adressen definieren.
E-Mails mit diesem Zeichensatz	Die Funktion prüft das Feld „charset“ in den Kopfzeilen (Header) der Mail auf die Zeichensätze, die in der angegebenen Liste eingetragen sind. E-Mails mit einem solchen Zeichensatz werden sofort als Spam klassifiziert.

Wenn Sie nur diejenigen Spams sofort löschen möchten, von denen Sie ganz sicher sein wollen, dass sie definitiv Spam sind, so stellen Sie die **Spam-Wahrscheinlichkeit** für **Hoch** auf 100 ein und definieren eine entsprechende Aktion. In diesem Fall werden nur die E-Mails in diesen Bereich fallen, bei denen die definitiven Kriterien (= die Blacklist oder Zeichensatz) eindeutig Spam festgestellt haben. Bei einer Einstellung von z.B. 91 bis 100 trifft es auch diejenigen Mails, bei denen Spam auch von anderen Kriterien mit höchster Wahrscheinlichkeit angenommen wird.

11.4.3 Praxistipps

Je nach konkreter Einsatzumgebung kann es sein, dass der Job bei einzelnen Kriterien auch in normalen und erwünschten Mails Spam-Hinweise zu erkennen meint, so dass solche E-Mails fälschlicherweise als Spams identifiziert und behandelt werden können. Sollten solche Fälle vorkommen, empfehlen wir die folgenden Konfigurationseinstellungen:

1. Liegen die betroffenen Mails immer knapp über dem Schwellwert, ab dem die Spam-Wahrscheinlichkeit beginnt, sollten Sie zunächst diesen Schwellwert etwas höher einstellen, um die Falsch-Klassifikationen zukünftig zu vermeiden.
2. Stehen Sie mit dem Absender von falsch klassifizierten E-Mails regelmäßig in Kontakt, sollten Sie ihn als Kontakt im Active Directory anlegen oder in die Whitelist (unter der Schaltfläche **Definitive Kriterien --> Definitive „Kein Spam“-Kriterien**) eintragen, so dass die Untersuchung dieser Mails künftig entfallen kann.
3. Versuchen Sie für Ihre Einsatzumgebung typische Business-Begriffe in den betroffenen Mails zu identifizieren und tragen Sie diese in die Business Words Wortliste ein. Der Job wird diese Wörter zukünftig über das kombinierte „Kein Spam“-Kriterium **HAM Phrasen im Nachrichtentext** berücksichtigen und Mails, die diese Wörter enthalten, weniger stark als Spam werten.

4. Trainieren Sie Ihren eigenen CORE Spam-Klassifikator. Siehe dazu “CORE Klassifikation” auf Seite 312.
5. Wenn trotz der Anpassungen 1 - 4 die Fehlklassifikationen sich nicht in einem akzeptablen Rahmen bewegen, sollten Sie z.B. mit Hilfe der Ursachenbeschreibung in der Quarantäne oder auch mit der Benachrichtigungs-Variable[30] **Details Spam-Analyse** herausfinden, welche Kriterien bei den falsch klassifizierten E-Mails Hinweise auf Spam geliefert haben. Handelt es sich wiederholt um dasselbe Kriterium, so ist dieses für Ihre Einsatzumgebung wahrscheinlich nicht aussagekräftig genug: Sie sollten dessen Bedeutung daher vermindern, indem Sie unter **Kombinierte Kriterien** seine **Kriterium-Relevanz** um eine Stufe verringern. So berücksichtigt der Job dieses Kriterium nicht mehr so stark bei der Bestimmung der Spam-Wahrscheinlichkeit.
6. Wenn Sie sich sehr gut mit den Merkmalen der bei Ihnen üblichen Mails (Spam und Nicht-Spam) auskennen, können Sie mit Hilfe der **kombinierten Kriterien** in **Erweiterte Konfiguration** auch die einzelnen Kriterien auf Ihre Einsatzumgebung hin optimieren. Dies kann vor allem dann sinnvoll sein, wenn Sie die Relevanz eines Kriteriums sehr weit verringern oder das Kriterium ganz ausschalten mussten, um False Positives auszuschließen. Die Kehrseite der Medaille kann eine spürbare Abnahme der Spam-Erkennung sein. Zu diesem Thema lesen Sie bitte Kapitel “Anti-Spam für Experten” auf Seite 300 aufmerksam durch.

11.4.4 Anti-Spam-Prüfung - Jobbeispiel

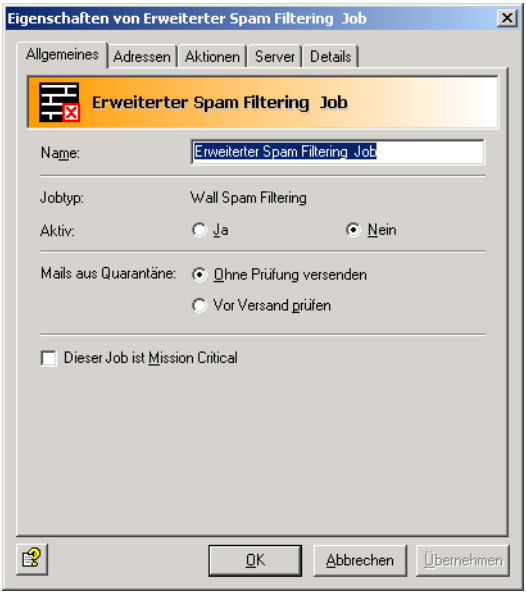
Unter **Richtlinien-Konfiguration --> Mail Transport Jobs** finden Sie einen Job für die Anti-Spam-Prüfung. Öffnen Sie **Erweiterter Spam Filtering Job** mit einem Doppelklick. Dieser Job untersucht die E-Mails auf spezielle Spam-Hinweise.

11.4.4.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre

30. siehe “Liste der Benachrichtigungsvariablen” auf Seite 101

Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130. Die Option **Mission Critical** finden Sie unter **Dieser Job ist Mission Critical** näher beschrieben.

In diesem Job ist der **Zusatz im Betreff** auf der Registerkarte **Aktionen** zu finden.

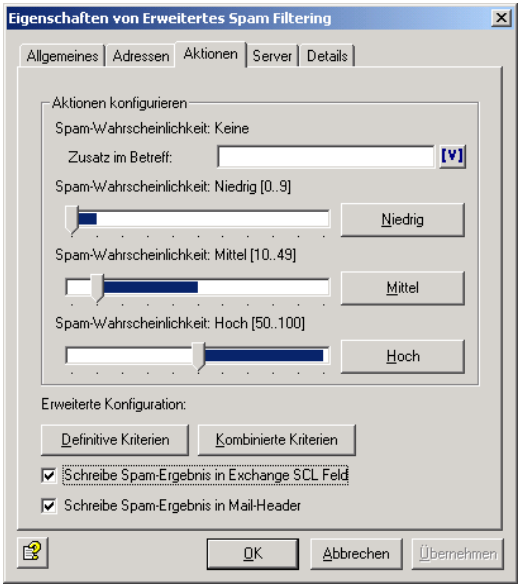
11.4.4.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhan-

denen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

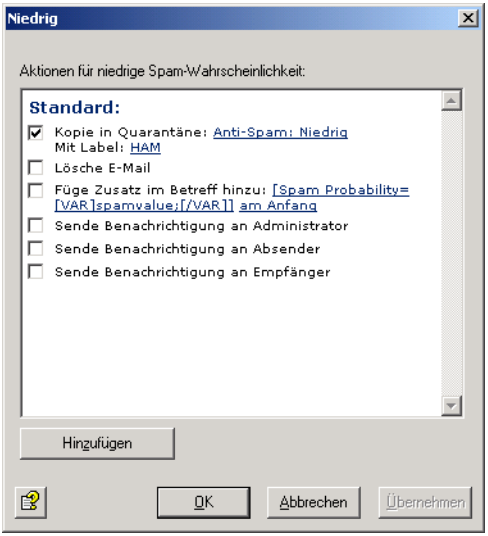
11.4.4.3 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, wie hoch die Spam-Wahrscheinlichkeiten sein sollen und was mit dem gefundenen Spam passieren soll.



In diesem Job sind folgende Spam-Wahrscheinlichkeiten eingerichtet:

1. Im Bereich **Spam-Wahrscheinlichkeit: Keine** (Wert = 0) werden normalerweise überhaupt keine Aktionen ausgeführt. Die einzig mögliche Aktion in diesem Wahrscheinlichkeitsbereich ist ein **Zusatz im Betreff**, den Sie direkt innerhalb dieser Registerkarte einrichten können. Denkbar wäre ein Zusatz wie „Anti-Spam checked“ o. ä.
2. Für den Bereich **Spam-Wahrscheinlichkeit: Niedrig** (hier eingestellt von 0 - 9) stellen Sie die Aktionen auf einer separaten Registerkarte ein. Klicken Sie dazu auf die Schaltfläche **Niedrig**. Sie erhalten folgenden Dialog:



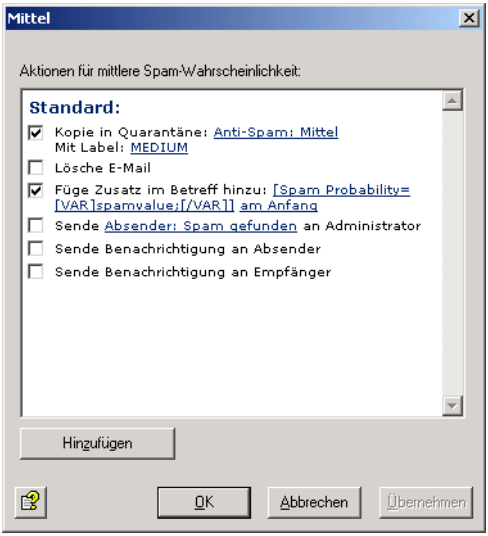
Als einzige Aktion wird eine Kopie in die Quarantäne gestellt. Die Mail wird dem Empfänger zugestellt und erhält in der Quarantäne das **Label** *HAM*.

Die Spam-Wahrscheinlichkeiten sind in diesem Job mit kleinen Werten belegt. Das bedeutet, dass bereits eine niedrige Wahrscheinlichkeit für Spam angenommen wird, wenn nur kleine Hinweise einiger Kriterien auf Spam gefunden wurde. In die beiden Spam-Wahrscheinlichkeitsbereiche **Keine** und **Niedrig** fallen so mit hoher Sicherheit nur geschäftsrelevante Mails (HAM). Die eingestellten Werte für **Niedrig** schließen die Wahrscheinlichkeit **Keine** ein. Daher werden die für **Niedrig** definierten Aktionen auch für die Wahrscheinlichkeit **Keine** ausgeführt. Durch die hier definierten Aktionen werden also alle Mails in den Quarantänen abgelegt. Dadurch kann eine HAM-Menge von Mails für das Trainieren eines eigenen CORE Klassifikators[31] erzeugt werden. Schalten Sie die Aktion wieder aus (Datenschutz!), wenn Sie die nötigen Mails für das CORE Training gesammelt haben.

3. Für die Konfiguration der Aktionen im Bereich **Spam-Wahrscheinlichkeit: Mittel** (hier eingestellt von 10 - 49) klicken Sie auf die Schaltfläche **Mittel**.

31. siehe "CORE Klassifikation" auf Seite 312

Sie erhalten folgenden Dialog:



Als Aktion wird eine Kopie in die Quarantäne gestellt. Die Mail erhält in der Quarantäne das **Label** *MEDIUM*. Die Original-Mail wird dem Empfänger zugestellt. Eine weitere Aktion ist der **Zusatz im Betreff**, der dem Empfänger die Spam-Wahrscheinlichkeit dieser E-Mail mitteilt (z.B. Spam-Wahrscheinlichkeit = 31). Je höher dieser Wert ist, desto mehr kann der Empfänger davon ausgehen, dass diese E-Mail nicht oberste Priorität hat. Die Spam-Wahrscheinlichkeit **Mittel** ist für diejenigen Mails gedacht, bei denen es unsicher ist, ob sie Spam sind oder nicht. Die niedrigen Werte dieser Einstellung bedeuten, dass eine mittlere Wahrscheinlichkeit für Spam angenommen wird, wenn nur einige Kriterien massive Hinweise oder aber viele Kriterien kleinere Hinweise auf Spam gefunden haben. Es ist empfehlenswert, diese Mails in einer eigenen Quarantäne (**Anti-Spam: Mittel**) zu sammeln und es den Anwendern zu überlassen, was mit diesen Mails geschehen soll.

Die Anwender können mittels Sammelbenachrichtigungen über die Spam-Mails einer Quarantäne informiert werden. Lesen Sie dazu "Quarantäne-Sammelbenachrichtigungen einrichten" auf Seite 111. Sie können die Mails auch mittels des Microsoft-SCL-Wertes durch den Exchange Store direkt in die Junk-Ordner der Anwender leiten lassen (siehe dazu auch nächsten Abschnitt). Durch den konfigurierten **Zusatz im Betreff** mit der Angabe des Spam-Wahrscheinlichkeitswerts kann jeder Anwender selbst mit einem Filter in Outlook die weitere Behandlung dieser Mails einrichten.

Schreibe Spam-Ergebnis in Exchange SCL Feld

Ab Service Pack 1 für Exchange 2003 und Outlook 2003 liefert Microsoft einen Spam-Filter aus. Dieser Intelligent Message Filter (IMF) ermittelt eine Wahrscheinlichkeit dafür, ob es sich bei einer E-Mail um Spam handelt. Das Ergebnis dieser Berechnung ist der so genannte Spam Confidence Level (SCL). Er kann ganzzahlige Werte zwischen -1 und 9 annehmen. Je größer der SCL, umso größer ist auch die Spam-Wahrscheinlichkeit. Ein SCL von 0 bedeutet, dass höchstwahrscheinlich keine Spam-Mail vorliegt, und -1 wird für E-Mails vergeben, auf die der Filter überhaupt nicht angewandt wurde, beispielsweise für interne Mails von Absendern aus der gleichen Exchange-Organisation. Der Exchange-SCL-Wert kann automatisch bestimmte Aktionen auslösen wie zum Beispiel die Weiterleitung in die Junk-Mail-Ordner der Anwender in Outlook 2003, ohne dass die Anwender selbst aktiv werden müssen. Im "Exchange System Manager" können Sie zentral definieren, was bei einem bestimmten SCL-Schwellenwert mit den Mails passieren soll. Dabei muss die Aktion nicht auf dem System festgelegt werden, das die Bewertung vornimmt. Da der IMF den SCL-Wert in die Mail schreibt, kann erst das Zielsystem die gewünschte Maßnahme ergreifen. Das Mail-Gateway muss hierfür ebenfalls mit Exchange 2003 betrieben werden.

Auch wenn Sie den IMF nicht nutzen können oder möchten, können Sie mit dieser Option den Spam-Wahrscheinlichkeitswert des Spam Filtering

Jobs als SCL-Ergebnis festlegen, so dass Sie die Exchange-Store-Funktionalität für die möglichen Aktionen bzw. Weiterverarbeitung nutzen können. Der Spam-Wahrscheinlichkeitswert wird intern in die SCL-Werte umgerechnet, so dass Outlook sie erkennen kann.

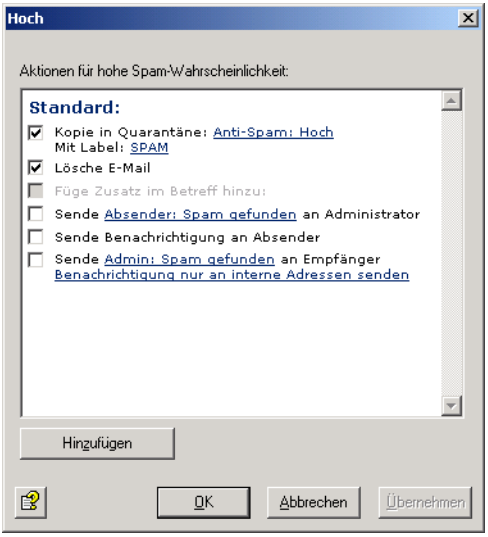
Wenn Sie die Sammelbenachrichtigungen nutzen, werden die Anwender über alle relevanten Spam-Mails informiert (siehe "Quarantäne-Sammelbenachrichtigungen einrichten" auf Seite 111). Sie können in diesem Fall auf die Verwendung der Exchange-Store-Weiterleitung in Junk-Mail-Ordner verzichten. Nähere Informationen über das Exchange-SCL-Feld erhalten Sie unter http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx

Schreibe Spam-Ergebnis in Mail-Header

Der Spam-Wahrscheinlichkeitswert wird für alle drei Spam-Wahrscheinlichkeiten (Niedrig, Mittel und Hoch) in den Mail-Header geschrieben. Dazu wird der Ergebniswert in eine Sternenkette umgerechnet (1 Stern beinhaltet einen Wert bis zu 10, 2 Sterne bis zu 20, 3 Sterne bis zu 30 ...), so dass darauf eine Outlook-Regel anwendbar ist. Sie können das Ergebnis auch für jede Spam-Wahrscheinlichkeit extra definieren, indem Sie unter der **Aktionen**-Registerkarte **Hinzufügen --> X-Header-Feld hinzufügen** wählen. In diesem Fall wird das Ergebnis nicht in eine Sternenkette umgerechnet, sondern direkt als Wert ausgegeben.

4. Für die Konfiguration der Aktionen im Bereich **Spam-Wahrscheinlichkeit: Hoch** (hier eingestellt von 50 - 100) klicken Sie auf die Schaltfläche **Hoch**.

Sie erhalten folgenden Dialog:



Die Spam-Wahrscheinlichkeit **Hoch** ist für diejenigen E-Mails gedacht, die wirklich Spam sind und daher nicht zugestellt werden sollen. Hier wird die Original-Mail sofort gelöscht und dem Empfänger nicht zugestellt. Eine Kopie der Mail geht in die Quarantäne. Angesichts des heutigen Spamaufkommens werden keinerlei Benachrichtigungen[32] an den Administrator versandt.

Bei hohem Mailaufkommen können die Quarantänen schnell sehr umfangreich werden und den E-Mail-Durchsatz belasten. Wenn Sie die Mails nicht mehr benötigen (beispielsweise für CORE Klassifikation), sollten Sie die Low- und High-Quarantänenkopie deaktivieren.

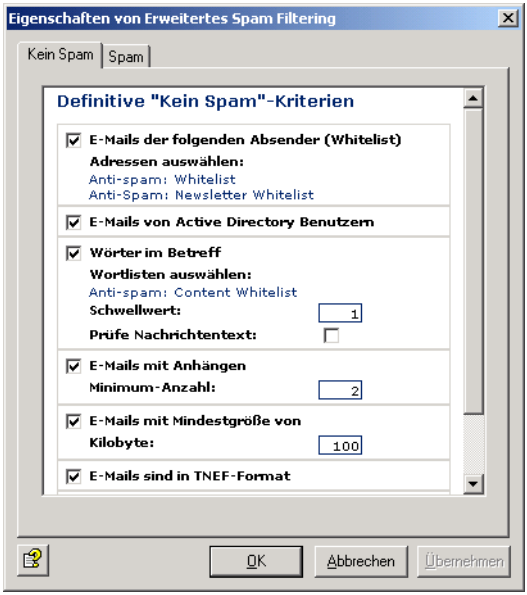
32. siehe dazu “Benachrichtigungsvorlagen erstellen” auf Seite 100

Es kann für Ihre Produktivumgebung durchaus vertretbar sein, die Wahrscheinlichkeiten für den **Mittel**- und **Hoch**-Bereich anders anzusetzen. Beobachten Sie aber am besten vorher einige Zeit, ob der Job mit diesen Einstellungen in Ihrer Produktivumgebung gute Ergebnisse erzielt.

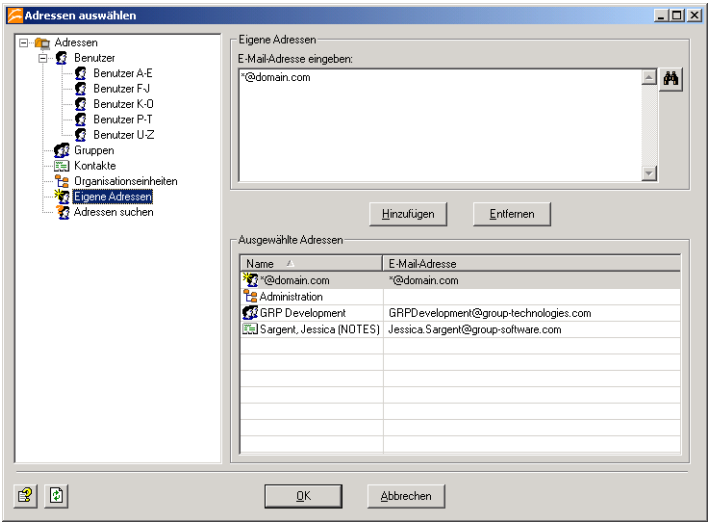
Ziel sollte sein:

- möglichst viele Spam-Mails in der **Anti-Spam: High**-Quarantäne
- möglichst viele Spam-Mails in der **Anti-Spam: Low**-Quarantäne
- und damit möglichst wenig E-Mails in **Anti-Spam: Medium**

Auf der Registerkarte **Aktionen** können Sie die Spam-Kriterien anpassen. Klicken Sie auf **Definitive Kriterien**. Sie erhalten folgenden Dialog:



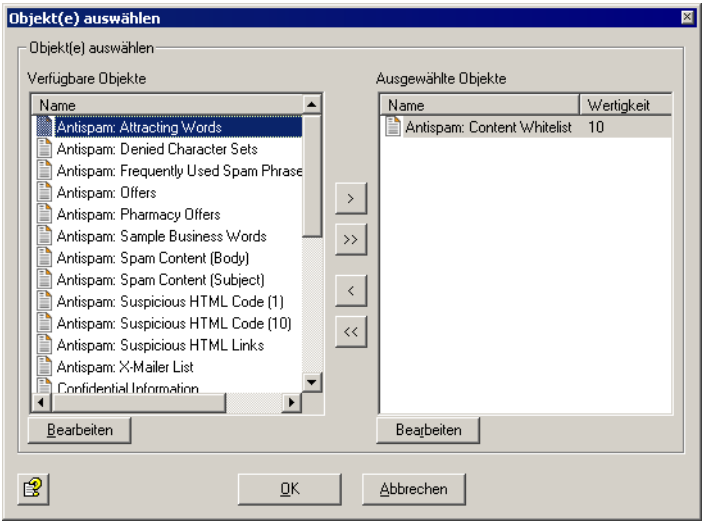
Wenn Sie E-Mails bestimmter Absender immer zulassen möchten, klicken Sie im Kriterium **E-Mails der folgenden Absender (Whitelist)** auf die Liste **Anti-Spam: Whitelist** und **Anti-Spam: Newsletter Whitelist**. Sie erhalten das Adressauswahlfenster:



Wählen Sie hier die Adressen aus oder geben Sie eigene E-Mail-Adressen an, die als Absender immer zugelassen werden sollen. Als Wildcards sind der Stern (*) und das Fragezeichen (?) zugelassen[33]. Sie können also z.B. auch nur Domänen in der Form **.domain.com* angeben. Klicken Sie nach der Eingabe Ihrer Adressen auf **OK**.

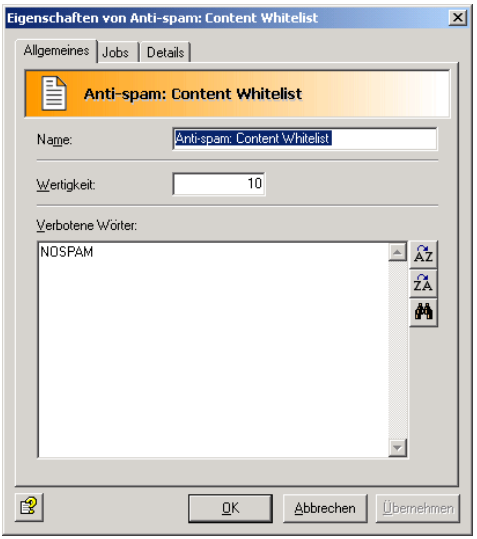
Nun können Sie im Dialog **Definitive „KeinSpam"-Kriterien** das nächste Kriterium **Wörter im Betreff** anpassen. Klicken Sie auf **Anti-Spam: Content Whitelist**. Sie erhalten den Dialog zur Auswahl der Wortlisten:

33. zu Wildcards in der Adressprüfung siehe "Adressprüfung" auf Seite 266



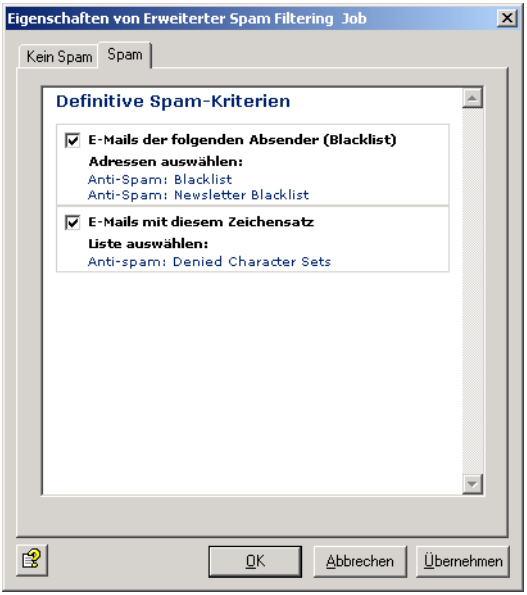
Mit den Pfeiltasten [>] und [<] können Sie der Liste Wortlisten hinzufügen und entfernen. Die Doppelpfeile fügen alle vorhandenen Wortlisten hinzu bzw. entfernen alle. Doppelklicken Sie im rechten Fenster auf **Anti-Spam: Content Whitelist** oder klicken Sie auf die Schaltfläche **Bearbeiten**.

Sie erhalten folgenden Dialog:



Weitere Informationen zur Einrichtung von Wortlisten finden Sie in "Wortlisten einrichten" auf Seite 272. Eine nähere Beschreibung der weiteren Kriterien finden Sie unter "Definitive Kein-Spam-Kriterien" auf Seite 285.

Nachdem Sie die Wortliste gefüllt und zwei Mal mit **OK** bestätigt haben, klicken Sie nun auf die Registerkarte **Spam**:



Klicken Sie im Feld **E-Mails der folgenden Absender (Blacklist)** auf die Liste mit **Anti-spam: Blacklist** und **Anti-spam: Newsletter Blacklist**. Sie erhalten wieder ein Adressauswahlfenster und können nun eigene E-Mail-Adressen oder Domänennamen hinzufügen.

Sowohl die Whitelist als auch die Blacklist sollte korrekt und aktuell gehalten werden!

Zusätzlich können Sie mit der Wahl eines bestimmten Zeichensatzes E-Mails bestimmter Regionen definitiv zum Spam erklären. Aktivieren Sie die Checkbox neben **E-Mails mit diesem Zeichensatz** und klicken Sie auf **Anti-spam: Denied Character Sets**. Jede Zeile enthält den Code für einen Zeichensatz. Die Zuordnung der einzelnen Länder zu einem Zeichensatz können Sie der Registerkarte

Details entnehmen. Sollten Sie Kommunikationspartner aus den Ländern haben, deren Zeichensätze in dieser Liste angegeben sind, so passen Sie die Liste folgendermaßen an:

1. Kopieren Sie die Liste **Anti-Spam: Denied Character Sets** unter **Basis-Konfiguration --> Wortlisten**.
2. Geben Sie Ihrer Liste einen neuen Namen.
3. Löschen Sie die Zeichensätze mit den Länder Ihrer Kommunikationspartnern aus der Liste heraus.
4. Speichern Sie die Liste ab.
5. Löschen Sie die Liste **Anti-Spam: Denied Character Sets** im Job **Erweitertes Spam Filtering** und setzen Sie Ihre eigene Liste unter **Definitive Spam-Kriterien --> E-Mails mit diesem Zeichensatz** ein.

Die Funktion prüft in der E-Mail ausschließlich das Header-Feld „charset“. Achten Sie darauf, dass Sie für diese Option nur die dafür bestimmten Zeichensatz-Liste(n) auswählen und keine andere Wortliste.

11.4.4.4 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

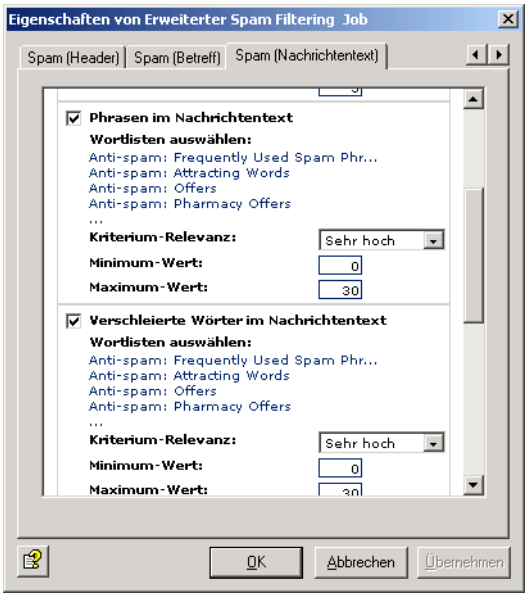
11.4.5 Anti-Spam für Experten

Im Spam-Filtering Job lassen sich definitive und kombinierte Spam-Kriterien einstellen. Die **definitiven Kriterien** bedeuten eine sofortige Entscheidung in die eine oder andere Richtung (Spam oder Nicht-Spam) und werden sofort mit dem Etikett „Spam-Wahrscheinlichkeit ist 0% = **Keine**“ oder „Spam-Wahrscheinlichkeit ist 100% = **Hoch**“ belegt. Die **kombinierten Kriterien** kommen nur für solche Mails zum Einsatz, für die die definitiven Kriterien nicht bereits entschieden haben. Für die eigentliche Spam-Erkennung mit kombinierten Kriterien werden mehrere Analysemechanismen (Kriterien-Untersuchungen) parallel durchgeführt und anschließend nach der Analyse der E-Mail miteinander „verrechnet“. Jedes Kriterium besitzt seine eigene **Relevanz** für das Gesamtergebnis (die individuelle

Wertigkeit dieses Kriteriums), die von **Niedrig** bis **Sehr hoch** eingestellt werden kann. Deaktiviert wird das Kriterium per Klick in der Checkbox. Außerdem lassen sich die meisten Kriterien noch mit einem individuellen Wert für **Minimum** und **Maximum** belegen. Diese beiden Werte beziehen sich z.B. auf die Wortlisten, gegen die das Kriterium die E-Mails prüft. Unterhalb des Minimum-Werts wird dieses Kriterium für die entsprechende E-Mail in der Gesamtwertung nicht berücksichtigt. Ist der Maximum-Wert erreicht, so ist **dieses Kriterium** der Meinung: „Das ist Spam!“.

Bitte Achtung: Die Aussage „Das ist Spam!“ gilt nur für das spezielle einzelne Kriterium, dessen Maximum-Wert durch die Analyse der E-Mail erreicht ist. Da es sich in dieser Spam-Analyse immer um eine Analyse mit kombinierten Kriterien handelt, können die anderen Kriterien auch „ganz anderer Meinung sein“ und beim gegenseitigen Verrechnen das einzelne Kriterium sozusagen „überstimmen“. Näheres finden Sie auch im unten stehenden Beispiel.

11.4.5.1 Kombinierte Kriterien - Beispiel



Sie benutzen im kombinierten Kriterium **Phrasen im Nachrichtentext** in der Registerkarte **Spam (Nachrichtentext)** u.a. die Wortliste **Anti-Spam: Frequently Used Spam Phrases**, um den Nachrichtentext aller eingehenden E-Mails auf Spam zu prüfen. Diese Wortliste ist mit der Wertigkeit 5 belegt. Wird in einer E-Mail nun ein Wort/Phrase dieser Wortliste gefunden, z.B. „check it out“, so wird es mit 5 bewertet und gezählt. Sie geben nun an, ab wie vielen Wörtern dieses Kriterium in der Gesamtwertung berücksichtigt werden soll (**Minimum-Wert**) und wann Ihr individuelles „Spam-Maß“ für dieses Kriterium voll ist (**Maximum-Wert**). Zählen Sie dazu die Wertigkeit der zu findenden Wörter zusammen. Wenn Sie hier also einen Wert von 30 angegeben (so wie in unserem vorkonfigurierten Job), so müssen in der Mail 6 verschiedene Wörter dieser Wortliste gefunden werden, um für dieses Kriterium voll als Spam klassifiziert zu werden, da die Wertigkeit der Wortliste und der darin enthaltenen Wörter = 5 ist. Werden hier beispielsweise nur 3 verschiedene Wörter gefunden, so ist diese Mail für dieses Kriterium noch nicht „voll“ Spam, aber die Wahrscheinlichkeit schon recht hoch. Von einer anderen Wortliste mit der Wertigkeit = 10 genügen natürlich bereits 3 Treffer für den „vollen“ Spam-Hinweis.

Mehrere gleiche Wörter werden nicht mehrfach, sondern nur einmal gezählt. Sollte also in diesem Beispiel in der E-Mail drei Mal der Begriff „check it out“ vorkommen, so zählt dieser Begriff insgesamt nur 5, nicht 15 (im Gegensatz zu einem normalen Wall Content Filtering Job).

Zusätzlich geben Sie die **Kriterium-Relevanz** an. Wenn Sie diese auf **Sehr hoch** eingestellt haben, wird das Kriterium in der Gesamtwertung entsprechend stark berücksichtigt.

11.4.5.2 Kombination der Hinweise zur Spam-Wahrscheinlichkeit

Die Einzelwertigkeiten aller kombinierten Kriterien werden anschließend entsprechend ihrer eingestellten Relevanz gewichtet und es wird eine Gesamtwertigkeit errechnet. Der Job vergleicht diese Gesamtwertigkeit (= Spam-Wahrscheinlichkeit der E-Mail) am Ende der Prüfung mit den drei individuell einzustellenden Schwellwerten und ordnet die E-Mail damit einem der vier Spam-Wahrscheinlichkeitsbereiche zu (**Keine** bis **Hoch**). Zusammen mit anderen kombinierten Kriterien kann also unsere Beispielmail mit den 3 gefundenen Wörtern aus der 5er

Wortliste dann in der Gesamtrechnung doch noch in den „Das ist Spam“-Bereich fallen.

In diesem Beispiel könnte unsere E-Mail mit den 6 gefundenen Wörtern der 5er Wortliste, die in diesem Kriterium den Stempel „Das ist voll Spam“ erhalten hat, durch die Aufrechnung mit anderen Kriterien aber auch die Spam-Wahrscheinlichkeit **Keine** oder **Niedrig** erhalten haben und damit am Ende im Gesamtergebnis den Stempel „Das ist wahrscheinlich kein Spam“.

Die Gesamtwertung entsteht erst aus den Kriterium-Relevanzen, den Minimum- und Maximum-Werten und den individuell eingestellten Spam-Wahrscheinlichkeitsbereichen.

Die einzelnen kombinierten Kriterien finden Sie unter **Erweiterte Konfiguration** auf vier Registerkarten.

Einen Überblick über die im Job enthaltenen kombinierten Kriterien geben die folgenden Tabellen. Bitte schlagen Sie für weiterführende Informationen zu kombinierten Kriterien im technischen Whitepaper nach oder wenden Sie sich an unseren Support.

11.4.5.3 Kombiniertes Kein Spam-Kriterium

Kriterium	Beschreibung
HAM-Phrasen im Nachrichtentext	Überprüft, ob sich Wörter aus dem typischen Business-Wortschatz der Anwender im Nachrichtentext der E-Mail befinden.

11.4.5.4 Kombinierte Klassifizierungskriterien

Hier werden Ergebnisse von anderen Spam-Erkennungsprodukten eingerechnet, von denen jedes oftmals als alleiniges Spam-Erkennungsmerkmal eingesetzt wird. Durch die Kombination mit anderen Kriterien im Wall Spam Filtering Job werden die spezifischen Nachteile der einzelnen Produkte eliminiert.

Kriterium	Beschreibung
CORE Klassifizierung siehe auch "CORE Klassifikation" auf Seite 312	Die Ergebnisse der CORE Klassifikation mit dem internen SPAM Klassifikator werden zur Berechnung der Spam-Wahrscheinlichkeit herangezogen. Der Rückgabewert wird als prozentuale Wahrscheinlichkeit zur Berechnung weitergegeben und mit sehr hoher Kriterium-Relevanz einbezogen (Standardeinstellung).
DCC-Prüfung siehe auch "Anti-Spam mit Wall DCC Spam Filtering" auf Seite 307	Die Ergebnisse der DCC-Prüfung durch den angegebenen DCC-Server werden zur Berechnung der Spam-Wahrscheinlichkeit herangezogen. Der Rückgabewert liefert eine Zahl oder „many" zur Berechnung zurück.
Exchange SCL Wert siehe auch "Definitive Kein-Spam-Kriterien" auf Seite 285 und "Schreibe Spam-Ergebnis in Exchange SCL Feld" auf Seite 293	Auch der Intelligent Message Filter (IMF) ermittelt eine Wahrscheinlichkeit dafür, ob eine E-Mail Spam ist. Das Ergebnis dieser Berechnung ist der so genannte Spam Confidence Level (SCL). Er kann ganzzahlige Werte zwischen -1 und 9 annehmen. Je größer der SCL, umso größer ist auch die Spam-Wahrscheinlichkeit. Ein SCL von 0 bedeutet dabei, dass höchstwahrscheinlich keine Spam-Mail vorliegt. Nähere Informationen siehe auch http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx

11.4.5.5 Kombinierte Header-Kriterien

Kriterium	Beschreibung
Suspekte Absendereigenschaften	Überprüft, ob der "From"-Header vorhanden und gefüllt ist und ob er mit dem Absender des SMTP-Protokolls übereinstimmt.
Suspekte Empfängereigenschaften	Überprüft, ob der "To"-Header vorhanden und gefüllt ist und ob sich mindestens einer der SMTP-Empfänger im "To"- oder "CC"-Header befindet.
Zahlen in Absenderadresse(n)	Überprüft, ob sich in einer der Absender-Adressen (SMTP oder Mail-Header) Ziffern in der E-Mail-Adresse befinden.
Anzahl Empfänger pro E-Mail	Überprüft die Anzahl der Empfänger einer E-Mail.
Bekannte Spam X-Mailer	Überprüft, ob es sich beim X-Mailer-Eintrag in der E-Mail um einen bekannten Spam-Mail-Client handelt.

11.4.5.6 Kombinierte Betreff-Kriterien

Kriterium	Beschreibung
Fehlender Betreff	Überprüft, ob das Betreff-Feld vorhanden und gefüllt ist.
Empfängeradresse im Betreff	Überprüft, ob sich der Teil vor dem @ einer Empfänger-Adresse im Betreff der Mail befindet.
Junk-Zeichenkette im Betreff	Überprüft, ob lange Zeichenketten von Versteckzeichen (**Leerzeichen**) und sinnlose Junk-Zeichenketten im Betreff der Mail vorkommen.
Phrasen im Betreff	Überprüft, ob sich Wörter aus dem typischen Spam-Wortschatz im Betreff der Mail befinden.

11.4.5.6 Kombinierte Betreff-Kriterien

Kriterium	Beschreibung
Verschleierte Wörter im Betreff	Überprüft, ob sich verschleierte Wörter aus der angegebenen Wortliste(n) im Betreff der Mail befinden.

11.4.5.7 Kombinierte Nachrichtentext-Kriterien

Kriterium	Beschreibung
Empfängeradresse im Nachrichtentext	Überprüft, ob sich der Teil vor dem @ einer Empfänger-Adresse im Nachrichtentext der Mail befindet.
Junk-Zeichenkette im Nachrichtentext	Überprüft, ob lange Zeichenketten von Versteckzeichen und sinnlose Junk-Zeichenketten im Nachrichtentext der Mail vorkommen.
Phrasen im Nachrichtentext	Überprüft, ob sich Wörter aus dem typischen Spam-Wortschatz im Nachrichtentext der Mail befinden.
Verschleierte Wörter im Nachrichtentext	Überprüft, ob sich verschleierte Wörter aus der angegebenen Wortliste(n) im Nachrichtentext der Mail befinden.
Suspekter HTML-Code	Überprüft, ob sich HTML-Konstrukte im Nachrichtentext der Mail befinden.
Suspekte HTML-Links	Überprüft, ob sich Spammer-Links im Nachrichtentext der Mail befinden.

11.4.6 Manuelle Anti-Spam-Konfiguration

Wenn Sie den oben beschriebenen Job **Wall Spam Filtering** nicht nutzen möchten, empfiehlt es sich, für eine effektive Anti-Spam-Konfiguration folgende Reihenfolge im Jobablauf einzurichten:

1. Adressprüfung auf bekannte Spam-Adressen.
2. Spam-Prüfung mittels DCC-Server. Siehe dazu das Kapitel “Anti-Spam mit Wall DCC Spam Filtering” auf Seite 307.

3. Betreffzeilenprüfung auf Text und auf Auffälligkeiten in der Formatierung, z.B. Punkte oder Leerzeichen. Siehe dazu die Wortliste **Spam Content (Subject)** in der **Basis-Konfiguration** unter **Wortlisten**.
4. Nachrichtentextprüfung auf Spam Links (z.B. auch auf Umleitungen[34] und Click tracker[35]). Siehe dazu die Wortliste **Spam-Links (Body)** in der **Basis-Konfiguration** unter **Wortlisten**.
5. Nachrichtentextprüfung auf Spam-Text und bekannte typische Auffälligkeiten wie z.B. HTML-Kommentare innerhalb eines HTML-Mailtextes. Siehe dazu auch die Wortliste **HTML Spam Detector** in der **Basis-Konfiguration** unter **Wortlisten**.
6. Spam-Prüfung mit CORE. Siehe dazu das Kapitel "CORE Klassifikation" auf Seite 312.

Achten Sie auf die richtigen Prioritäten der Jobs, um die Prüfungen möglichst effektiv und performanceoptimiert durchzuführen.

11.5 Anti-Spam mit Wall DCC Spam Filtering

11.5.1 Was ist DCC?

Die DCC-Prüfung basiert auf der Technologie des Distributed Checksum Clearinghouse (DCC). DCC ist ein weltweites Anti-Spam Netzwerk von Benutzern und Servern, die zur Zeit über 150 Millionen E-Mails pro Tag analysieren. Dabei werden ständig für auffällige Massen-E-Mails intelligente Prüfsummen gebildet. Die iQ.Suite analysiert anhand dieser Prüfsummen eingehende E-Mails.

Streng genommen entdeckt das Distributed-Checksum-Clearinghouse-Verfahren nicht nur Spam, sondern allgemein massenhaft versandte E-Mails (Bulk-Mails). In einem DCC-Verbund ermittelt die iQ.Suite zu jeder eingehenden E-Mail spezielle Prüfsummen und sendet diese an einen Server (Clearinghouse). Dieser antwortet mit der Angabe, wie oft diese Mail-Prüfsumme bereits registriert wurde und erhöht gleichzeitig den entsprechenden Zähler. DCC-Server tauschen wie-

34. Übliche bekannte Umleitungsservices und typische Umleitungsbefehle wie http://redir.+ und Ähnliches unter Benutzung von Wildcards in der Wortliste.
35. Click tracker sind Webseiten mit integrierten Skripten, die jeden Klick auf den Spam-Link überprüfen (wer, wann, woher ...), bevor auf die entsprechende Seite weitergeleitet wird.

derum untereinander entsprechend den Vorgaben ihrer Betreiber Daten über die gezählten Bulk-Mails aus.

Entscheidend für das Funktionieren von DCC ist der Gebrauch von "Fuzzy Checksums": Normalerweise sind Prüfsummenalgorithmen derart konstruiert, dass sie ein völlig anderes Ergebnis liefern, sobald sich auch nur ein Bit in der zugehörigen Nachricht ändert. Da Spam-Versender häufig zufällige Komponenten in ihre Mails einbauen, um einer Kategorisierung zu entgehen oder Nachrichten zu personalisieren, benötigt DCC eine andere Art von "Fingerabdruck", bei dessen Erstellung bestimmte Teile der Nachricht unberücksichtigt bleiben. Diese "unscharfen" Prüfsummen sind so angelegt, dass sie für E-Mails mit gleicher Aussage dasselbe Ergebnis liefern und zufällige Anteile möglichst unberücksichtigt lassen.

Die DCC Prüfsummen-Abfrage erfolgt in Echtzeit, so dass immer die aktuellsten Spam-Pattern genutzt werden. Ein Update der Spam-Pattern im Sinne eines Herunterladens auf die lokalen E-Mail Server ist somit nicht erforderlich.

DCC integriert sich nahtlos in die bestehenden Anti-Spam-Analysemethoden der iQ.Suite. Die iQ.Suite erhält als Antwort die Häufigkeit, mit der dieselbe Nachricht bei den teilnehmenden Servern eingegangen ist. Eine E-Mail mit einem hohen "bulk count", also entsprechend hoher Verbreitung, ist entweder Spam oder eine Nachricht aus einer populären Mailing-Liste. Da dieses System prinzipiell Spam-Mails und Mailinglisten-Mails (Newsletter, tausendfach versandte Kundenbriefe etc.) nicht unterscheiden kann, sollte es nur in Kombination mit Whitelists eingesetzt werden.

Da außerdem bei ähnlichen Mails die gleichen Prüfsummen erzeugt werden können, ist es möglich, dass auch geschäftsrelevante E-Mails als Massenmails identifiziert werden können. Eine weitere Schwäche ist, dass bei einer Spam-Welle die ersten Spam-Mails noch nicht als Massen-Mails erkannt werden, da ganz am Anfang die Zählerstände noch nicht hoch genug sind. Je mehr DCC-Benutzer die Prüfsummen an den Server melden, desto genauer wird das Ergebnis für weitere Anfragen anderer Benutzer.

Wegen der genannten Schwächen ist die DCC-Prüfung im Jobtyp **Wall Erweitertes Spam Filtering** als kombiniertes Kriterium eingebunden und sollte als separater Job nur zu Testzwecken eingesetzt werden.

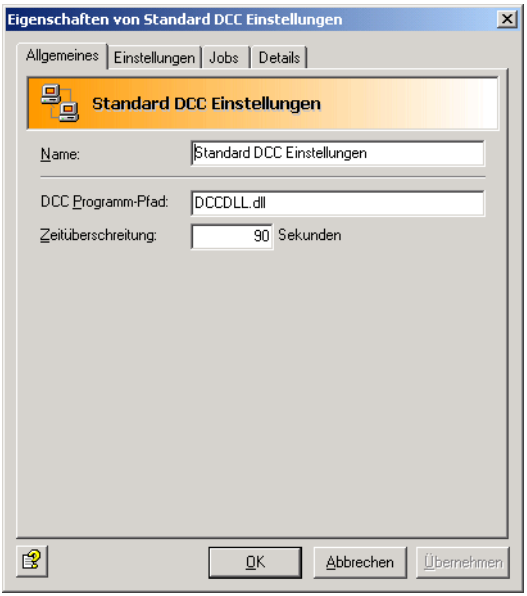
Für die Verwendung von DCC ist ein "DCC Connector" erfordlich. Der Connector ist integraler Bestandteil der iQ.Suite und steht nach der Installation automatisch zur Verfügung. Dieser Connector erstellt die jeweiligen Checksummen und stellt die Verbindung zu dem DCC-Netzwerk her. Er empfängt die Ergebnisse des DCC-Netzwerkes und übergibt die Informationen an den jeweiligen iQ.Suite Job.

Nähere Informationen über DCC und eine Liste von verfügbaren Servern finden Sie unter: http://www.rhyolite.com/anti-spam/dcc/

11.5.2 Konfiguration der DCC-Einstellungen

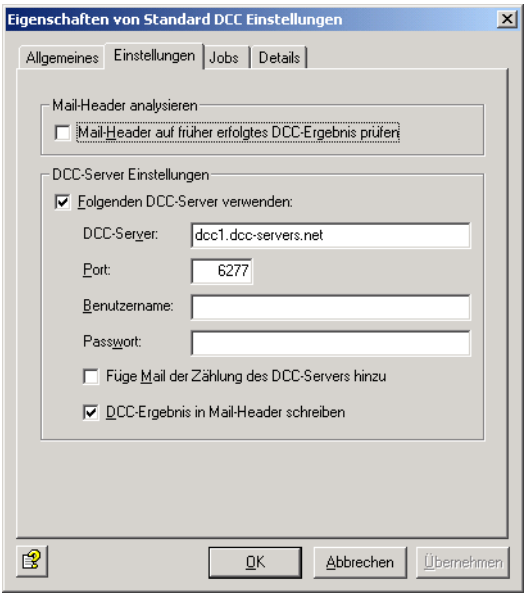
Die Standard-DCC-Einstellungen sind fertig konfiguriert. Eigene DCC-Einstellungen sind möglich.

1. Klicken Sie auf **Basis-Konfiguration --> Utility-Einstellungen --> DCC**
2. Wählen Sie im rechten Fensterbereich die **Standard-DCC-Einstellungen** mit einem Doppelklick aus. Sie erhalten folgende Ansicht:



Die Pfad zur DLL ist immer der Gleiche und sollte nicht geändert werden!

3. Wählen Sie die Registerkarte **Einstellungen**. Hier können Sie den verwendeten DCC-Server und dessen Parameter einstellen[36].



a) Folgenden DCC-Server verwenden:

Freie DCC-Server verwenden das Protokoll UDP über IP-Port 6277 des DCC-Server und benötigen in der Regel keine Authentifizierung. Schalten Sie den Port 6277 für UDP an der Firewall frei.

Hinter manchen DNS-Namen, wie zum Beispiel "dcc1.dcc-servers.net", stehen mehrere Server mit unterschiedlichen IP-Adressen. Berücksichtigen Sie das bei Ihrer Firewall-Konfiguration.

b) Mail-Header auf früher erfolgtes DCC-Ergebnis prüfen

Mit dieser Option wird nicht bei einem DCC-Server angefragt, sondern die E-Mail wird auf ein bereits früher als X-Header eingetragenes

36. siehe auch "Was ist DCC?" auf Seite 307

Ergebnis eines DCC-Servers geprüft. Setzen Sie diese Option, wenn die Mail bereits auf dem SMTP-Gateway durch einen DCC-Job geprüft wurde. Auf den nachfolgenden Mail-Servern ist es anschließend ausreichend, das X-Header-Feld auf dieses Ergebnis zu untersuchen. (siehe dazu auch Option unter d)).

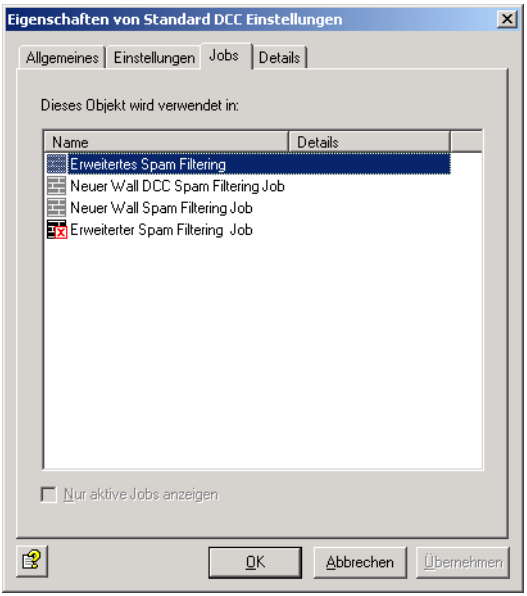
c) Füge Mail der Zählung des DCC-Servers hinzu

Hier legen Sie fest, ob der DCC-Server Ihre Anfrage mitzählen soll. Der Job übermittelt dem DCC-Server die Prüfsummen der Mail, so dass eventuelle weitere Anfragen anderer DCC-Benutzer exakter ausfallen.

d) DCC-Ergebnis in Mail-Header schreiben

Die Antwort eines DCC-Servers besteht aus einem charakteristischen Text, den die iQ.Suite als X-Header in die untersuchte E-Mail einträgt. So können Sie das Ergebnis auch auf nachfolgenden Systemen auswerten (siehe dazu auch Option unter b)).

4. Unter der Registerkarte **Jobs** werden alle Jobs aufgelistet, in denen die DCC-Prüfung verwendet werden kann.



11.5.3 Anti-Spam mit DCC - Jobbeispiel

Nutzen Sie den Jobtyp **Wall DCC Spam Filtering**, um die Funktion des DCC-Servers zu testen. Im Produktivbetrieb empfiehlt es sich, die DCC-Prüfung im Job **Erweitertes Spam Filtering** einzuschalten. Siehe hierzu "Was ist DCC?" auf Seite 307 und "Kombinierte Klassifizierungskriterien" auf Seite 304.

1. Klicken Sie auf **Richtlinien-Konfiguration --> Mail Transport Jobs**.
2. Wählen Sie mit der rechten Maustaste **Neu --> Wall DCC Spam Filtering**.
3. Vergeben Sie auf der Registerkarte **Allgemeines** einen Namen und schalten Sie den Job **Aktiv**. Näheres zur Option **Mails aus Quarantäne** finden Sie in "Aus Quarantäne senden" auf Seite 130. Schalten Sie die Option **Dieser Job ist Mission Critical** aus.
4. Richten Sie die Adresseinstellungen unter **Adressen** ein. Siehe hierzu "Adresslisten" auf Seite 90.
5. Stellen Sie unter **DCC-Optionen** einen **Schwellwert** ein. Wenn dieser Wert überschritten ist, wird der Job die Mail als Spam einsortieren. Der Wert entspricht dem Zählerstand, den der DCC-Server zurückmeldet. Beispiel: Schwellwert = 100 bedeutet, dass die Mail als Spam kategorisiert werden soll, sobald der DCC-Server 100 gleiche Prüfsummen registriert hat.
6. Lassen Sie unter **Aktionen** die Mail mit dem Label *DCC* in die Quarantäne stellen und konfigurieren Sie eine Administrator-Benachrichtigung, damit Sie die Ergebnisse verfolgen können.
7. Die Auswahl der **Server** und die Eingabe der Job **Details** wird wie in der Beschreibung zu "Server auswählen" auf Seite 233 und "Details zum Job eingeben" auf Seite 233 durchgeführt.
8. Klicken Sie auf **OK**. Der Job ist nun aktiviert.

11.6 CORE Klassifikation

11.6.1 Übersicht

Bei der Inhaltsanalyse auf der Basis der CORE Technologie werden die Inhalte durch eine Repräsentation von Text als Vektor „angelernt", so dass später auch Mails mit Texten gleicher Kategorie gefunden werden können, ohne dass sie

explizit in einer Wortliste vorkommen. CORE ist unabhängig von Wortlisten und funktioniert in allen europäischen Sprachen.

Insbesondere bei der Spam-Abwehr bietet sich dieses Verfahren an, da Spam-Versender oft mit ständig wechselnden (auch nicht existenten) Adressen und neuen Inhalten arbeiten. Für die Spam-Kategorisierung werden die Mails in SPAM und HAM eingeteilt und ein SPAM-Klassifikator erstellt. Die iQ.Suite beinhaltet einen sorgfältig trainierten SPAM-Klassifikator, der sofort einsetzbar ist. Werden die Mails in mehrere verschiedene, selbst zu definierende Kategorien wie beispielsweise Support, Sales, Anfragen usw. sortiert, kann CORE die Mails nach diesem Inhalt klassifizieren und ermöglicht dadurch eine inhaltsbasierte Weiterverarbeitung. Sie können einen solchen Klassifikator individuell für Ihr Unternehmen trainieren.

Um Mails und Dokumente mit CORE zu analysieren, werden zunächst die vorhandenen Mails des Unternehmens (alle Spam und Nicht-Spam-Mails: Business Mails, Newsletter, Angebote, Anfragen usw.) im iQ.Suite Monitor in den CORE Klassifikator kopiert. Der Klassifikator ist im Monitor sichtbar, sobald ein neuer **CORE Klassifikator** unter **Basis-Einstellungen** angelegt worden ist. Der Klassifikator wird trainiert und kann anschließend im **Wall CORE Classification** Job verwendet werden. Sollte das Analyseergebnis durch den Job nicht zu Ihrer Zufriedenheit ausfallen, können Sie den Klassifikator jederzeit „nachtrainieren“, indem Sie neue Mails zu den einzelnen Kategorien hinzufügen.

11.6.2 CORE für Anti-Spam verwenden

11.6.2.1 Standard-Job einschalten

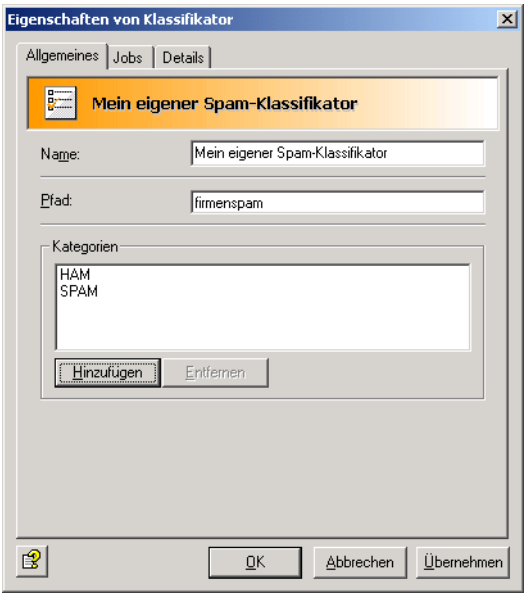
Schalten Sie den Job **Erweiterter Spam Filtering** aktiv. Dieser Job beinhaltet eine Spam-Prüfung mit dem mitgelieferten CORE Spam Klassifikator.

Dieser Klassifikator kann nicht geändert oder erweitert werden und wird bei der Installation an anderer Stelle gespeichert als selbst erstellte Klassifikatoren!

11.6.2.2 Eigenen Spam-Klassifikator im Standard-Job verwenden

Wenn Sie CORE für Anti-Spam mit einem eigenen Spam-Klassifikator verwenden möchten, hier die Schritte im Einzelnen:

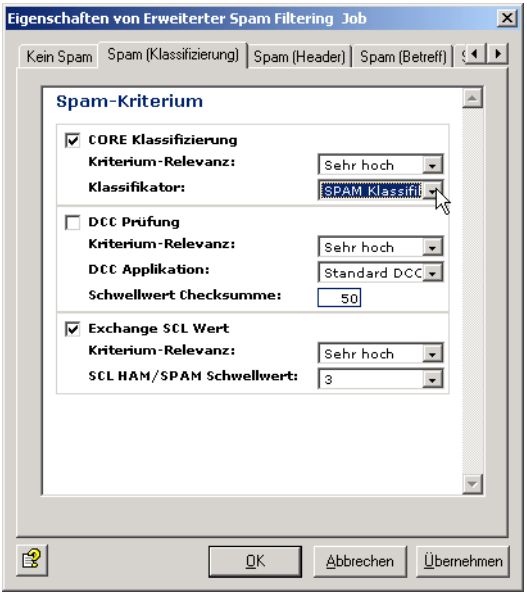
1. Legen Sie unter **Basis-Konfiguration --> Utility-Einstellungen --> CORE Klassifikatoren** einen neuen Klassifikator mit 2 Kategorien an:



   Geben Sie dem Klassifikator einen Namen und bestimmen Sie den Namen des Ordners, der unter `iQ.Suite\GrpData\Quarantine\` angelegt werden soll. Geben Sie hier nur den Ordnernamen an und verwenden Sie innerhalb des Ordnernamens keine Sonderzeichen!

2. Speichern Sie die Konfiguration -->
3. Aktualisieren Sie den **iQ.Suite Monitor** mit der rechten Maustaste --> **Aktualisieren**.
4. Kopieren Sie die Mails per Drag & Drop aus den **Quarantänen** in den CORE Klassifikator und ordnen Sie sie der passenden Kategorie zu.
5. Trainieren Sie den Klassifikator im **iQ.Suite Monitor** durch rechte Maustaste --> **Alle Tasks --> Klassifikator anlernen**. Nach erfolgreichem Training werden unterhalb des angelegten Klassifikator-Ordners Log-Dateien abgelegt und der Status im **iQ.Suite Monitor** ändert sich. Im Event Viewer erhalten Sie eine Meldung.
6. Öffnen Sie den **Erweiterter Spam Filtering** Job in der **Richtlinien-Konfiguration --> Mail Transport Jobs** durch einen Doppelklick.

7. Klicken Sie auf die Registerkarte **Aktionen**.
8. Klicken Sie auf die Schaltfläche **Kombinierte Kriterien**.
9. Wählen Sie die Registerkarte **Spam (Klassifizierung)**.
10. Setzen Sie Ihren eigenen **Klassifikator** ein:



11. Klicken Sie **OK** und noch einmal **OK**.
12. Speichern Sie die Konfiguration -->

Jetzt verwendet der Spam-Job den von Ihnen erstellten Klassifikator. Diesen Klassifikator können Sie jederzeit nachtrainieren.

Beachten Sie beim Nachtrainieren eines Spam-Klassifikators:

Fügen Sie keine „beliebigen“ E-Mails zu den Klassifikatoren hinzu. Das sind beispielsweise Spam-Mails, die zur Verschleierung viele „gute“ Wörter enthalten, und die Sie der Spam-Menge zuordnen oder Newsletter, die Werbebotschaften enthalten und die Sie der Ham-Menge zuschlagen.

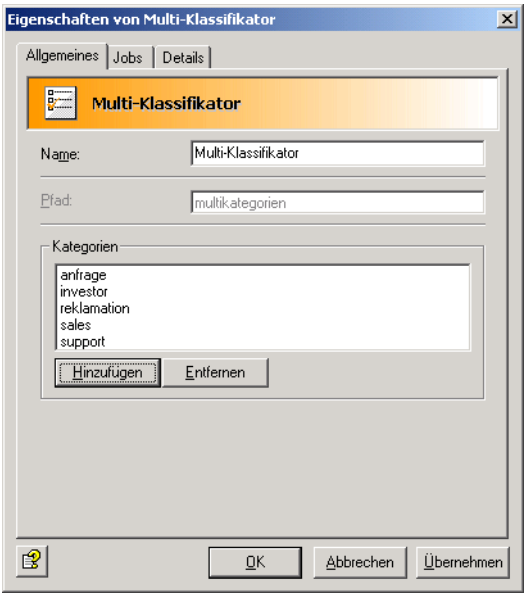
11.6.3 CORE für Inhaltsklassifizierung verwenden

Beispiel einer Unternehmensrichtlinie: E-Mails an die Adresse info@company.com sollen automatisch nach Inhalt in verschiedene vorher definierte Kate-

gorien eingeteilt werden und ebenfalls automatisch an die richtigen Adressaten weitergeleitet werden.

Dazu legen Sie einen CORE Job mit einem eigenen Klassifikator und mit mehreren Kategorien an:

1. Legen Sie unter **Basis-Konfiguration --> Utility-Einstellungen --> CORE Klassifikatoren** einen neuen Klassifikator mit mehreren Kategorien an:



   Geben Sie dem Klassifikator einen Namen und bestimmen Sie den Namen des Ordners, der unter `iQ.Suite\GrpData\Quarantine\` angelegt werden soll. Geben Sie hier nur den Ordnernamen an und verwenden Sie innerhalb des Ordnernamens keine Sonderzeichen!

2. Speichern Sie die Konfiguration -->
3. Aktualisieren Sie den **iQ.Suite Monitor** mit der rechten Maustaste --> **Aktualisieren**.
4. Kopieren Sie die Mails per Drag & Drop aus den **Quarantänen** in den CORE Klassifikator und ordnen Sie sie der passenden Kategorie zu.
5. Trainieren Sie den Klassifikator im **iQ.Suite Monitor** durch rechte Maustaste --> **Alle Tasks --> Klassifikator anlernen**. Nach erfolgreichem Trai-

ning werden unterhalb des angelegten Klassifikator-Ordners Log-Dateien abgelegt und der Status im **iQ.Suite Monitor** ändert sich. Im Event Viewer erhalten Sie eine Meldung.

6. Erstellen Sie mehrere **Wall CORE Classification** Jobs mit diesem CORE Klassifikator und schalten Sie sie aktiv (siehe dazu Neuer CORE Classification Job - Jobbeispiel).
7. Speichern Sie die Konfiguration -->

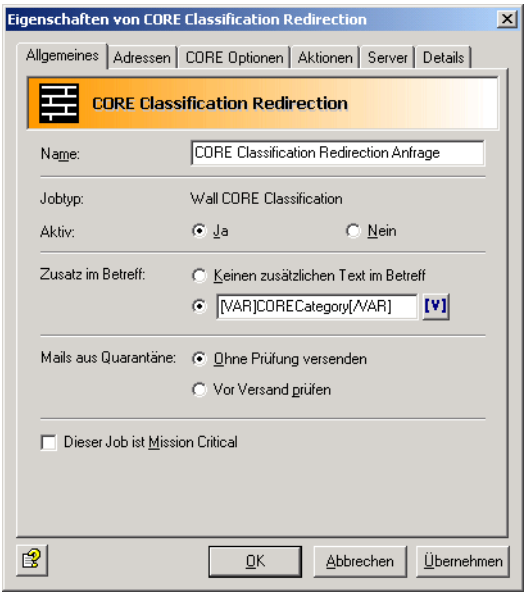
Jetzt werden die Mails nach Inhalten klassifiziert. Die Weiterverarbeitung wie zum Beispiel eine Weiterleitung der Mails an die richtigen Adressaten definieren Sie im **CORE Classification** Job unter **Aktionen**.

11.6.3.1 Neuer CORE Classification Job - Jobbeispiel

Wählen Sie unter **Richtlinien-Konfiguration --> Mail Transport Jobs --> Neu --> Wall CORE Classification** Job aus.

11.6.3.1.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie unter **Name** einen eigenen Namen für den Job vergeben. Da es ein neuer Job ist, wird er sofort **Aktiv** geschaltet.



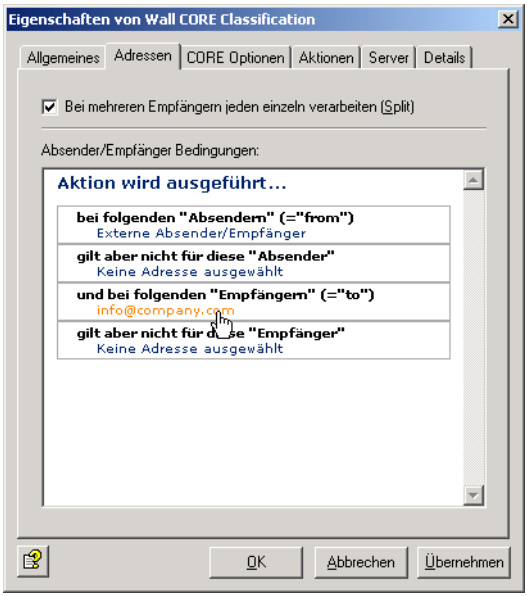
Vergeben Sie als **Zusatz im Betreff** die Variable für das CORE Klassifizierungsergebnis: [VAR]CORECategory[/VAR]. Dieser Zusatz wird in den Betreff jeder Mail eingefügt, deren Inhalt durch CORE klassifiziert und weiterverarbeitet worden ist. Dadurch weiß der Empfänger, dass diese Mail automatisch inhaltsbasiert an ihn umgeleitet wurde.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130.

11.6.3.1.2 Adressbedingungen einrichten

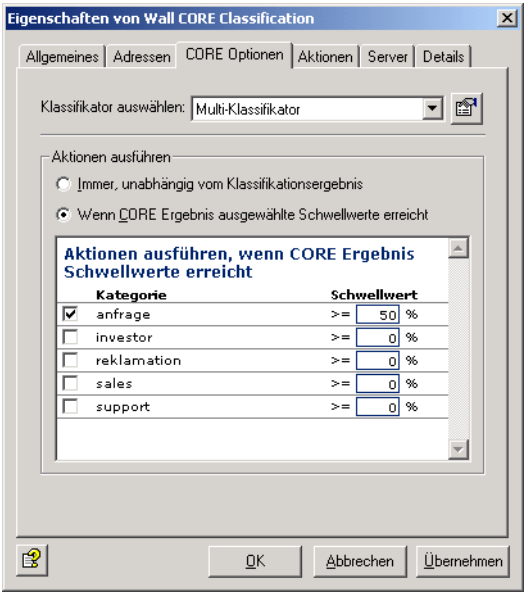
Klicken Sie auf die Registerkarte **Adressen**. Definieren Sie unter **bei folgenden „Absendern“** die Externen Absender und stellen Sie die gewünschte „info“-Adresse unter **und bei folgenden „Empfängern“** ein:



Mehr über Adressen erfahren Sie unter “Adresslisten” auf Seite 90.

11.6.3.1.3 CORE Optionen einstellen

In der Registerkarte **CORE Optionen** wählen Sie den oben erstellten Klassifikator aus. Die darin enthaltenen Kategorien werden angezeigt:



Jetzt definieren Sie eine Aktion für den Fall, dass die E-Mail als **Anfrage** klassifiziert wurde. Für alle Mails oberhalb eines Schwellwertes von 50% treten die definierten Aktionen in Kraft. Bei allen anderen Mails erfolgt keine Aktion.

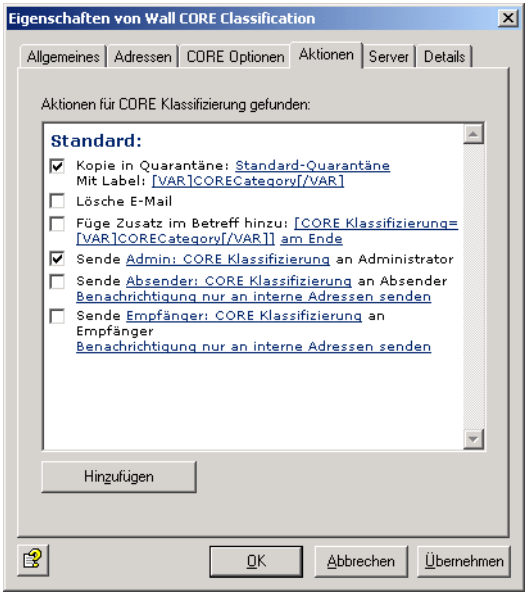
Die Option **Immer, unabhängig vom Klassifikationsergebnis** führt jede konfigurierte Aktion aus, egal in welche Kategorie die Mail eingeteilt wurde. Wählen Sie diese Option beispielsweise dann, wenn

- Sie alle Mails mit der zugehörigen Kategoriebezeichnung in die Quarantäne stellen wollen (dafür wird ein **Label** mit einer Variablen gesetzt),
- Sie einen X-Header setzen wollen, der das **CORE Klassifizierungsergebnis** oder die **CORE Klassifizierungskategorie** enthält,
- Sie alle Mails mit einem **Zusatz im Betreff** versehen und dann den Empfängern zustellen lassen wollen.

Mit solchen Aktionen ist es möglich, die Weiterverarbeitung der Mails über Outlook-Regeln oder andere Anwendungen gezielt zu steuern.

11.6.3.1.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine E-Mail zu über 50% als Anfrage klassifiziert hat.



Damit Sie prüfen können, ob CORE die Klassifizierung korrekt durchgeführt hat, wird die E-Mail in die Quarantäne gestellt und eine Benachrichtigung an den Administrator gesendet. Im Produktivbetrieb können Sie diese beiden Aktionen ausschalten. Definieren Sie nun mit der Schaltfläche **Hinzufügen** die Aktion **Mail umleiten**:

Klicken Sie auf **Weiter**:

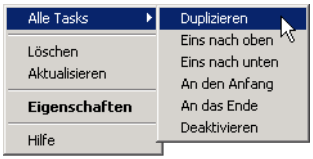
Geben Sie die E-Mail-Adresse der Abteilung oder der Person ein, die in Ihrem Unternehmen die Anfragen bearbeitet. Nähere Informationen zur Adresseingabe finden Sie unter “Adresslisten” auf Seite 90. Klicken Sie auf **Fertigstellen**.

11.6.3.1.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

11.6.3.2 Job duplizieren

Duplizieren Sie den Job, indem Sie ihn markieren und **Alle Tasks --> Duplizieren** wählen:



11.6.3.3 Einstellungen für alle anderen Kategorien wiederholen

Öffnen Sie die Kopie mit einem Doppelklick, vergeben Sie wieder einen sprechenden Namen und wiederholen Sie den Vorgang für Mails der nächsten Kategorie, die Sie ebenfalls an den zuständigen Adressaten weiterleiten lassen. Legen Sie jeweils einen Job für jede umzuleitende Kategorie an.

11.7 Limitieren der Anzahl der Empfänger

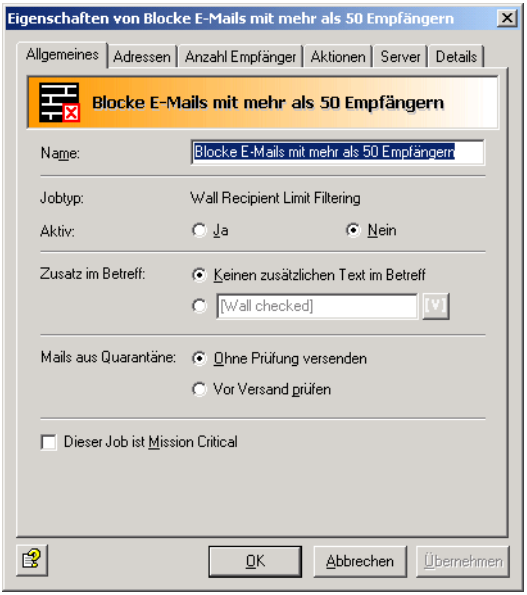
Dieser Jobtyp ermöglicht die Begrenzung auf eine gewisse Anzahl von Empfängern pro E-Mail. Ist dieser Job aktiv, ist es nicht möglich, unnötige Massenmails an alle Mitarbeiter des Unternehmens zu versenden.

11.7.1 Empfängeranzahl begrenzen - Jobbeispiel

Unter **Richtlinien-Konfiguration** finden Sie den Job **Blocke E-Mails mit mehr als 50 Empfängern**. Ziehen Sie diesen Job per Drag & Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

11.7.1.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Dass der Job inaktiv ist, erkennen Sie sofort am roten Kreuz unten in der Ecke des Job-Symbols. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert und das rote Kreuzsymbol verschwunden.



Der **Zusatz im Betreff** ist vordefiniert auf **Wall checked**. Dieser Zusatz wird, sofern aktiviert, in den Betreff jeder Mail eingefügt, wenn die Empfängerzahl kleiner als 50 ist.

Dieser Job bearbeitet keine Mails, die aus der **Quarantäne** wieder versendet werden, selbst wenn beim Versand aus der Quarantäne die Sende-Option **E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen** aktiviert wurde. **Ohne Prüfung versenden** bedeutet, dass dieser Job bei einem Mail-Versand aus der Quarantäne übergangen wird.

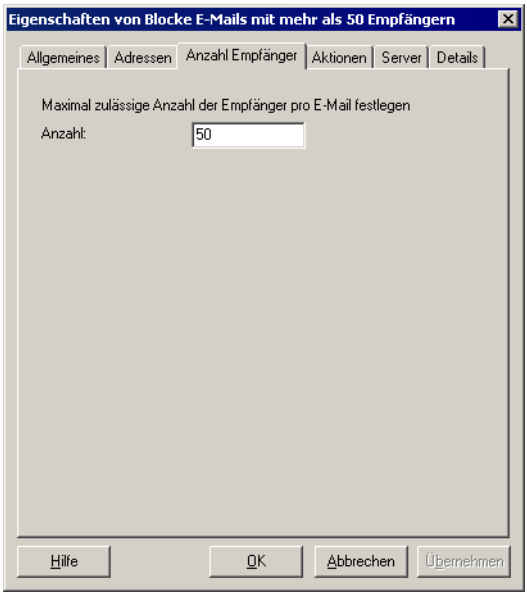
Näheres zum erneuten Versand aus der Quarantäne finden Sie in “Aus Quarantäne senden” auf Seite 130.

11.7.1.2 Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in “Adresslisten” auf Seite 90.

11.7.1.3 Anzahl Empfänger festlegen

In der Registerkarte **Anzahl Empfänger** geben Sie die maximale Anzahl von Empfängern pro E-Mail an:

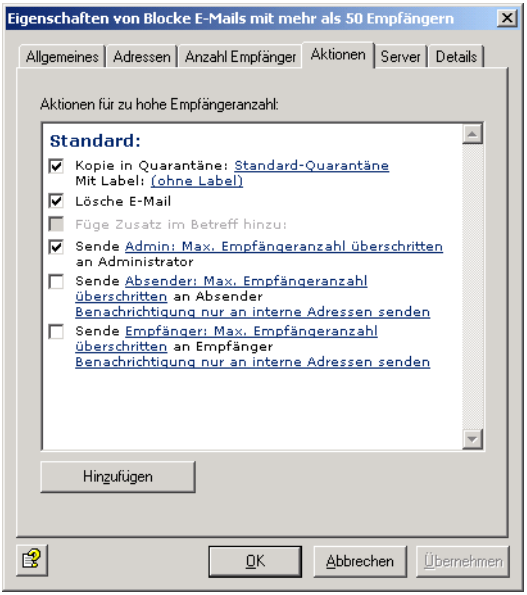


Jede ein- und ausgehende E-Mail darf also an maximal 50 Empfänger adressiert sein. Sobald eine Mail an 51 Empfänger adressiert ist, wird die definierte Aktion ausgelöst.

Sollten die Mails an eine Liste von Empfängern adressiert sein, die in einer einzigen Adresse zusammengefasst sind, so muss der Exchange-Server die Liste in die verschiedenen Empfänger auflösen können, um die Anzahl der Empfänger zu erkennen. Eine Adresse, die eigentlich eine Mailingliste ist, gilt als ein einziger Empfänger, wenn sie außerhalb der Reichweite des Exchange-Servers liegt.

11.7.1.4 Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine E-Mail mit zu vielen Empfängern gefunden hat.



Als Aktion wird eine Kopie der E-Mail in die Quarantäne gestellt und die betroffene E-Mail gelöscht. Das beinhaltet, dass die Mail den Empfängern **nicht** zugestellt wird. Eine Benachrichtigung über die Anzahl der Empfänger wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder mit HTML-Formatbefehlen gestaltet werden.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in „iQ.Suite Watchdog --> Virenprüfung einschalten - Jobbeispiel: Aktionen festlegen“.

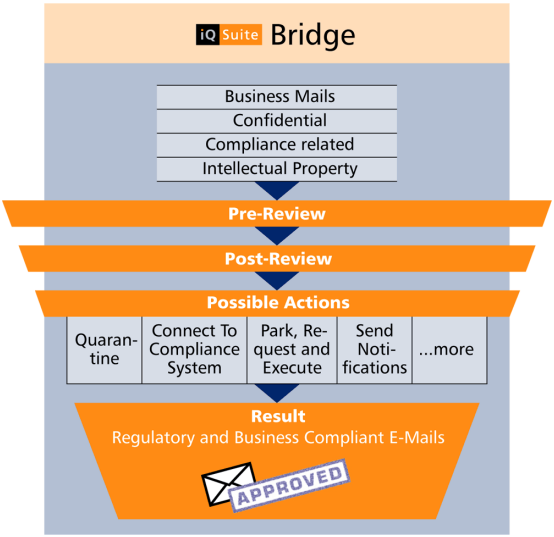
11.7.1.5 Server auswählen / Job Details

Die Auswahl der Server und die Eingabe der Job Details wird wie in der Beschreibung zu “Server auswählen” auf Seite 233 und “Details zum Job eingeben” auf Seite 233 durchgeführt.

12 iQ.Suite Bridge

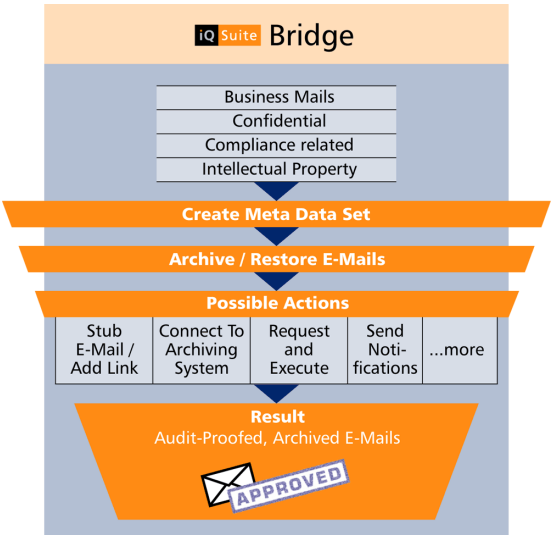
iQ.Suite Bridge ist die Schnittstelle, die Ihre E-Mail-Umgebung mit CRM-, ERP- und Archivierungssystemen verbindet.

Mit iQ.Suite Bridge erfüllen Sie die Anforderungen an Regulatory Compliance wie SOX, HIPAA, GDPdU, etc. und unterziehen alle eingehenden und ausgehenden E-Mails einer Prüfung. Dabei werden die beiden Modi Pre-Review (vor Zustellung) und Post-Review (nach Zustellung) sichergestellt. Ihre individuellen Richtlinien und eine automatisierte Klassifizierung garantieren, dass nur geschäftsrelevante E-Mails dem Review-Prozess zugeführt werden. Die Klassifikationsergebnisse und weitere Zusatzinformationen werden an das Compliance-System übergeben und dort direkt ausgewertet. Die Interaktion der iQ.Suite mit Ihrem Compliance-System ermöglicht eine gesetzeskonforme Weiterverarbeitung von E-Mails gemäß der Bewertung des jeweiligen Prüfergebnisses.



Mit iQ.Suite Bridge erfüllen Sie die Auflagen zur E-Mail-Archivierung und bilden diesen Prozess regelbasiert ab. Mit dem Schnittstellen- und Integrationsmodul ist es erstmals möglich, eine E-Mail-Archivierung auf der Grundlage fein abstimmbarer Richtlinien zur Vorverarbeitung, Filterung und Klassifizierung von E-Mails auf-

zubauen. Außerdem stellen Sie gesetzeskonforme Langzeitarchivierung gemäß den Unternehmensrichtlinien sicher. Sie integrieren eine flexible Gesamtlösung, welche die vielfältigen Auflagen bis ins Detail erfüllt.



Nähere Informationen über iQ.Suite Bridge finden Sie im separaten iQ.Suite Bridge Solution Guide, der in Kürze auf der Dokumentations-Website zur Verfügung steht.

13 Glossar

ACL (Access Control List)

Liste von Einträgen zu einem Objekt, das Zugangsberechtigungen steuert.

Active Directory

(AD). Verzeichnis für alle Netzwerkobjekte (Benutzer, Postfächer usw.). Der Verzeichnisdienst für Windows 2000 Server. Er speichert Informationen zu Objekten im Netzwerk und stellt diese Informationen autorisierten Administratoren und Benutzern zur Verfügung. Active Directory erlaubt Netzwerkbenutzern mit einem einzigen Anmeldevorgang den Zugriff auf alle Ressourcen im Netzwerk, für die sie Berechtigungen besitzen. Administratoren wird eine intuitive, hierarchische Ansicht des Netzwerks und ein einziger Verwaltungsort für alle Netzwerkobjekte zur Verfügung gestellt.

Active Directory Connector (ADC)

Ein Windows 2000-Dienst, der das Exchange 5.5-Verzeichnis mit Active Directory repliziert. Auf diese Weise kann ein Verzeichnis entweder aus Active Directory oder mit dem Verzeichnisdienst von Exchange 5.5 verwaltet werden.

Active/Active Clustering

Exchange 2000 läuft gleichzeitig auf mehreren Servern, siehe auch Server.

API

Application Programming Interface; Softwareschnittstelle, die es ermöglicht, Programmfunktionen aufzurufen und Daten auszutauschen.

Archive

Siehe Komprimierung.

ASP

Application Service Provider; Anbieter von IT-Services quasi "aus der Steckdose" zu einem vereinbarten Preis.

asymmetrisches Verfahren

Das Public-Private-Key-Verfahren: Dabei werden zwei Schlüssel verwendet, ein Public Key und ein Private Key. Die beiden bilden ein Schlüsselpaar. Jeder Absender braucht den Public Key jeden Empfängers. Die Schlüssel sind ver-

schieden, deshalb wird das Verfahren asymmetrisch genannt. Der Public Key wird öffentlich bekannt gegeben für den Fall, dass der Empfänger nur noch verschlüsselte E-Mail empfangen will. Der Empfänger entschlüsselt die E-Mails mit seinem Private Key, der nur ihm selbst zugänglich ist.

Auswahlregeln

Auswahlregeln grenzen die Anzahl der E-Mails oder Datenbanken ein, die durch die iQ.Suite geprüft werden sollen. Die Regeln filtern die Mails und Datenbanken nach firmeneigenen, selbst festzulegenden Richtlinien und ermöglichen so eine optimale Gewährleistung des firmeneigenen Sicherheitskonzeptes, siehe auch Regel.

Authentifizierung

Authentifizierung bezeichnet ein Verfahren, das prüft, ob eine Person berechtigt ist, auf bestimmte Dienste zuzugreifen. Eine Methode basiert auf dem Einsatz sogenannter digitaler Signaturen. Siehe digitale Signatur.

Authentizität

Mit der Authentizität wird die Echtheit einer Schrift oder Urkunde bezeichnet. Der Begriff wird auch für Echtheit elektronischer Dokumente verwendet -> authentisch, echt.

Back Office

Allgemeiner Ausdruck für Geschäftsbereiche eines Unternehmens, die für die Bearbeitung von Geschäftsdaten und Korrespondenz zuständig sind (z.B. Sekretariat, Auftragsbearbeitung).

Bitmap

Ein Bitmap ist ein unkomprimiertes Bildformat für pixelorientierte Grafiken und Fotos. Ein Faxserver benutzt Bildformate zur Darstellung des Faxes. Zerlegt man eine Bilddatei in Zeilen und Spalten, erhält man eine Rastergrafik. Jeder Punkt wird mit seiner Farbinformation als Bitfolge gespeichert. Das gleichnamige Dateiformat (Dateien vom Typ *.BMP) ist im Internet nicht verbreitet, da es keine Kompression erlaubt. Grafiken, im GIF- oder JPEG-Format gespeichert, reduzieren die Datenmenge gewaltig.

Business-to-Business

Elektronische Interaktion, Kommunikation und Handel zwischen Unternehmen.

Business-to-Customer

Elektronische Interaktion, Kommunikation und Handel zwischen Unternehmen und Kunden.

CA

Certification Authority. Siehe Zertifizierungsstelle.

Client

Allgemeiner Begriff für Computer und Anwendungsprogramme, die auf die Dienste und Ressourcen eines Servers zugreifen.

Client/Server-Systeme

Der Server ist eine Software, die einen Dienst (Service) zur Verfügung stellt und ein Client ist eine Software, die diesen Dienst benutzt. Diese Dienste können auf einem einzigen Computer zusammenarbeiten oder auch ein Netzwerk sein, bestehend aus mindestens einem zentralen Computer (Server), der seine Daten, Programme und gegebenenfalls andere angeschlossene Geräte einem oder mehreren anderen Computern (Clients) zur Verfügung stellt.

Content Security

Die Verwaltung und Kontrolle des Inhalts digitaler Mitteilungen. Content Security-Produkte schützen Computernetzwerke und Benutzer gegen Gefahren, die zufällig oder absichtlich in die Inhalte von E-Mails oder Übertragungen aus dem Internet eingebettet wurden.

CRL

Certificate Revocation List. Rückruf- oder Sperrliste für Zertifikate. Sofern die Angaben in einem Zertifikat während dessen Gültigkeitsdauer ungültig geworden sind, muss dieses Zertifikat ungültig gemacht werden. Da Zertifikate digitale Dokumente sind, lassen sie sich nicht einziehen oder vernichten. Deshalb werden auf einem weiteren Dokument, der sogenannten Sperrliste, alle ungültigen Zertifikate aufgeführt. Ein Standard für Sperrlisten ist im X.509-Protokoll definiert.

Customizing

Anpassung von Softwarelösungen an kundenspezifische Anforderungen.

Datenintegrität

Die Daten sind authentisch, d.h. sie wurden weder manuell noch maschinell unautorisiert verändert.

DHCP

Dynamic Host Configuration Protocol - Serververwaltung von IP-Adressen. Dabei handelt es sich im ein Protokoll, mit dem ein Server und seine Clients Informationen über die Konfiguration eines TCP/IP-Netzes austauschen können. DHCP wird zum Beispiel für die dynamische Zuweisung von IP-Adressen innerhalb eines LANs verwendet.

digitale Signatur

Das Gegenstück zu einer handschriftlichen Unterschrift für Dokumente, die in digitaler Form vorliegen; diese soll Sicherheit bei den folgenden Fragestellungen erbringen: - Die Authentizität, d.h. die Sicherheit über den Absender des Dokumentes. - Die Integrität des Dokumentes soll gewährleistet werden. - Die Verbindlichkeit; d.h. der Absender soll die Erstellung nicht bestreiten können. Diese Eigenschaften können mit Hilfe asymmetrischer Verfahren (--> asymmetrisches Verfahren) erreicht werden: Mit Hilfe des privaten Schlüssels (--> privater Schlüssel) werden Informationen erzeugt, anhand derer eine dritte Person sich unter Kenntnis des zugehörigen öffentlichen Schlüssels (--> öffentlicher Schlüssel) von der Korrektheit überzeugen kann.

DNS (Domain Name Service)

Das DNS ordnet den logischen Namen von Rechnern im Internet eine IP-Adresse zu.

Domäne

Auch "Domain". Die Domäne ist ein Teil bzw. Ebene in einer Adresse, den Konventionen (Rechtsbestimmungen) des DNS (Domain Name Service) folgend. In der Adresse werden die Domänen voneinander jeweils durch einen Punkt getrennt, z.B. www.group-technologies.com. In einem Domänennamen sind Buchstaben des Alphabets und Ziffern erlaubt. Als einziges Sonderzeichen kann der Bindestrich weltweit uneingeschränkt verwendet werden. Deutsche Umlaute sind seit einiger Zeit zwar erlaubt, aber nicht empfehlenswert (ausländische Tastaturen ohne Umlaute) und sollten wie beim Kreuzworträtsel) ersetzt werden (ä ->

ae, ö->oe, ü->ue). Der Name muss aus mindestens 3 Zeichen bestehen und dabei mindestens einen Buchstaben enthalten, da er sonst mit einer IP-Adresse verwechselt werden könnte.

Dynamic Link Library

Deutsch: Dynamische Verweis Bibliothek, frei übersetzt: Laufzeitbibliothek. Abgekürzt DLL. DLLs sind Bibliotheken unter Windows, die e enthalten, die erst dann (dynamisch) nachgeladen werden, wenn sie während der Ausführung einer Applikation benötigt werden. Diese Technik wird nicht nur dazu verwendet, Arbeitsspeicher zu sparen, sondern bietet in erster Linie die Möglichkeit, allgemein zugängliche Bibliotheken mit fertigen (Standard-)Objekten einzurichten, auf die bei der Entwicklung von Softwareprodukten zurückgegriffen werden kann.

E-Business

Electronic Business; Geschäftsprozesse, Abläufe und Kommunikation, die auf elektronischem Wege abgewickelt werden. Von einfachen Textverarbeitungsprogrammen über E-Mail bis hin zu komplexen Datenbanken und weltweiter Vernetzung werden Arbeiten in der Wertschöpfungskette elektronisch durchgeführt.

E-Business-Enabling

Das Schaffen von Voraussetzungen für E-Business.

E-Business-Organization

Die regelbasierte Organisation von eingehenden, ausgehenden sowie im System befindlichen Informationen im E-Business.

E-Business-Security

Der regelbasierte Informationsschutz und die Sicherstellung von Datenintegrität im E-Business.

E-Mail

Elektronische Post; Kommunikationsart, welche die elektronische Übertragung von Informationsobjekten (Texte, Sprache, Bilder, Grafiken etc.) ermöglicht.

E-Mail-Account

Registriertes Elektronisches Postfach.

Elektronisches Postfach

Eingerichteter E-Mail-Eingangs- und Ausgangskorb mit Berechtigungen zur Verwaltung für nur einen bestimmten Benutzer auf einem E-Mail-Server.

EMH (Enterprise Message Handler)

Schnittstelle zwischen der GROUP Basistechnologie und den einzelnen Modulen.

Entpacker

Programm zur Entkomprimierung von Dateien. Siehe auch Komprimierung.

False Positives

Fälschlich als Spam klassifizierte erwünschte E-Mail.

Filter

Siehe Regel.

Fingerprint

Identifiziert eine Datei durch Überprüfung des Inhalts der Datei oder, falls dies nicht möglich ist, durch ein Dateinamensmuster, zum Beispiel die Dateinamenserweiterung (Extension). Dadurch ergibt sich eine Kennzeichnung, vergleichbar mit einem individuellen Fingerabdruck. Das liefert die Grundlage dafür, Dateien gezielt zu verbieten oder zu erlauben. Sie können die Dateimuster selbst anlegen, mit deren Hilfe Watchdog den Dateityp eines Dateianhangs identifiziert.

Freeware

Kostenlos erhältliche Software, meist zum Herunterladen aus dem Internet oder auf Muster-CDs.

Frontend-/Backend-Konfiguration

Separate Gruppen von Servern für das Handling von Protokollen (POP3, etc.) und Datenspeichern (Data Stores). Dabei greifen die Clients auf Frontend-Protokollserver zu, die sich ihrerseits einer nach dem anderen mit Backend-Datenbankservern verbinden, um die gewünschten Daten abzufragen.

GIF

Steht für Graphics Interchange Format. Von CompuServe entwickeltes Standard-Format des WWW. Das GIF-Format komprimiert Bilddateien mit einer Farbtiefe von 256 Farben (8 Bit pro Pixel). Komprimierte Dateien entlasten die Netze und

erlauben schnellere Übertragungszeiten. Im Gegensatz zum JPEG-Format werden Farbübergänge scharf dargestellt. Interlaced-GIF-Dateien, eine Variante des GIF-Formats, erlauben während des Ladevorgangs schon eine grobe Vorschau. Bei Bilddateien ab dem Format GIF89a (noch eine GIF-Variante) kann eine Farbe als Alphakanal definiert werden, d.h. diese Farbe erscheint transparent, was die Platzierung auf WWW-Seiten mit farbigem Hintergrund erlaubt. Siehe dazu auch Komprimierung.

Globale Einstellungen

Allgemeine Einstellungen, gültig für die gesamte iQ.Suite.

Grabber

Bearbeitungsmodul für E-Mails. Der Grabber bearbeitet die E-Mails, die über jenen Exchange-Server versendet werden, auf dem der Grabber installiert ist, direkt auf dem Server. Der Grabber ruft für jede E-Mail die entsprechend konfigurierten Funktionsmodule (z.B. iQ.Suite Watchdog) auf.

Groupware

Software zur Unterstützung von Arbeitsgruppen durch Informations- und Kommunikationstechnik. Sie beinhaltet integrierte Lösungen für E-Mail, Gruppenkalender und -terminplaner, Informationsaustausch, elektronische Konferenzen sowie Dokumenten- und Arbeitsablaufmanagement.

Hotline

Zentrale Einrichtung für telefonischen Kundenservice.

HTML

HyperText Markup Language. Beschreibungs-/Darstellungssprache zur einfachen Erstellung von Hypertext-Dokumenten im WWW. HTML basiert auf SGML (Standard Generalized Markup Language), einer ISO Norm zur Definition von strukturierten Datentypen. Eine gute Beschreibung von HTML finden Sie unter http://selfhtml.teamone.de/.

Hyperlink

Ein Hyperlink ist ein Verweis (Sprungmarke) in einem Dokument auf eine andere Stelle in demselben oder in einem anderen Dokument, auch auf Seiten im Internet, die mit der Maus angesteuert werden kann.

IAB

Internet Activities Board - Koordinationsstelle von Forschungsarbeiten im Internet, teilt sich in IETF und IRTF.

IETF

Internet Engineering Task Force, Standardisierungsinstanz für Internet Standards.

Implementierung

Die Realisierung eines Entwurfs oder Konzepts durch ein lauffähiges Programm.

Informationsspeicher für Öffentliche Ordner

Der Teil des Informationsspeichers, der Informationen in Öffentlichen Ordnern verwaltet. Ein Informationsspeicher für Öffentliche Ordner setzt sich aus einer Rich-Text-Datei (.EDB-Datei) und einer systemeigenen Streaming-Internetinhaltdatei (.STM-Datei) zusammen, siehe auch MIME.

Informationsspeicher (Information Store)

Speichertechnologie, die von Exchange 2000 zum Speichern der Postfächer und Ordner von Benutzern verwendet wird. Es existieren zwei Arten von Speichern: Postfachspeicher und Informationsspeicher für Öffentliche Ordner.

Infrastruktur

Im Groupwareumfeld die Gesamtheit aller Hard- und Softwarekomponenten, Kommunikationseinrichtungen sowie organisatorischer Maßnahmen, die zum Betreiben z.B. eines Groupwaresystems notwendig sind.

Installierbares Dateisystem (Installable File System - IFS)

Eine Speichertechnologie, die als Archivierungssystem fungiert. Sie macht Postfächer und Öffentliche Ordner über Win32-Standardprozesse wie beispielsweise Microsoft Internet Explorer und die Eingabeaufforderung als traditionelle Ordner und Dateien verfügbar, siehe auch Web Storage System.

Integrated Collaborative Environment Software

Siehe Groupware.

Internet

Internet ist der Sammelbegriff für ein weltumspannendes Informationsnetz (World Wide Web) und der damit verbundenen Technologie auf der Basis spezieller

Standards, die das Netz unabhängig von Hardware und Betriebssystemen machen.

Internet Information Server (IIS)

Ein Microsoft Web Server. IIS ermöglicht Internetfunktionen von der Webseitenerstellung bis zur Entwicklung von serverbasierten Webapplikationen. IIS unterstützt die meisten Internetprotokolle wie NNTP, FTP und SMTP. Exchange 2000 erweitert die IIS-Fähigkeiten zusätzlich und benutzt den Server für das Message Routing.

Intranet

Unternehmensinternes Daten- und Kommunikationsnetz für den Informationsaustausch basierend auf der Internet-Technik ("privates Internet"). Anwendungen sind z.B. gemeinsam genutzte Datenbanken, Infopools oder Telefonverzeichnisse.

IP-Adresse

Eindeutige Internet-Protokoll-Adresse (Internet-Protocol-Address), wird als Protokoll der Netzwerkschicht im Internet verwendet und stellt die Adressierung zwischen den Partnerrechnern her. Die Adresse wird dargestellt durch eine Reihe von Ziffern, zum Beispiel 129.13.64.5.

IRTF

Internet Research Task Force. Teil des IAB, der langfristige technische Weiterentwicklungen des Internet betreut.

ISO

Abkürzung für International Standards Organisation. Internationales Normungsgremium. Von der ISO wurde das OSI-Modell zur Netzwerkübertragung entwickelt.

ISP

Internet Service Provider; ermöglicht dem Endkunden den Zugang zum Internet und bietet entsprechende Dienste an. ISPs verwalten die Internetzugangspunkte (points-of-presence).

ISP/ASP

-siehe ISP und ASP

IT

Informationstechnologie; umfasst alle Technologieformen, die für die Erstellung, Speicherung, den Austausch und Gebrauch von Informationen in all ihren Ausprägungen genutzt werden.

Job

Ein Job legt eine Abfolge von Aktionen fest, die bei einem bestimmten Ereignis oder nach gewissen Regeln in Gang gesetzt werden. Ein Job kann aktiv oder inaktiv sein. Ein inaktiver Job ist zwar vorhanden, aber nicht eingeschaltet. Für jedes Modul können mehrere Jobs erstellt werden. Diese werden dann modulübergreifend über die dem Job zugewiesene Priorität abgearbeitet.

JPEG

Auch JPG. Abkürzung für Joint Photographic (Experts) Group Format und wird "dschai-päck" gesprochen. JPG ist das Standard-Format des WWW für photorealistische Bilder. Das JPEG-Format komprimiert Bilddateien bis zu einer Farbtiefe von 16 777216 Farben (24 Bit pro Pixel). Komprimierte Dateien entlasten die Netze und erlauben schnellere Übertragungszeiten. Das JPEG-Format eignet sich im Gegensatz zum GIF-Format besonders zum Speichern von fotorealistischen Bildern mit vielen Farbnuancen. Dabei werden visuell nicht wahrnehmbare Datenverluste bewusst in Kauf genommen, um hohe Kompressionsraten zu erzielen. Gescannte Fotos oder Bilder von digitalen Kameras werden häufig im JPEG-Format gespeichert. Auch wird das JPEG-Format bevorzugt von Fax-Servern eingesetzt.

Junk-Mail

Jede Form unverlangter E-Mails, die den Empfänger nicht interessiert (Aufforderungen zur Besichtigung von Webseiten, Bilder, Kettenbriefe, Scherz-Viruswarnungen, Werbung für "make money faster" usw.). Junk-Mails kosten Unternehmensressourcen und den Empfänger zusätzlich Bearbeitungszeit, siehe auch Spam (wird oft ähnlich benutzt).

Komprimierung

Dateien werden in der Größe "zusammengestaucht" und/oder zusammengefasst, damit sie das Netz nicht belasten, besser und schneller versandt werden und/oder Speicherplatz sparen können. Es gibt verschiedene (auch selbstextrahie-

rende) Komprimierungsarten, z.B.: ZIP, TAR, ARJ, GZip, ARC, LZH. Auf verschiedenen Computersystemen werden unterschiedliche Arten verwendet. Unix verwendet vorzugsweise GZip und TAR, PC-Systeme ZIP und ARJ (siehe auch Packer). In solchen Dateien (Archive) können sich jedoch sehr leicht Viren verstecken, vor allem, wenn die Datei mehrere Male komprimiert wurde. Um sicher zu stellen, dass die Archive keine Viren enthalten, müssen daher Content Security-Werkzeuge in der Lage sein, rekursive Analysen durchzuführen, d.h. die Dateien wiederholt zu "entpacken", um sie in ihrem Ursprungszustand überprüfen zu können.

Konsole

Eine Sammlung von Verwaltungstools in MMC (Microsoft Management Console), die Objekte wie Snap-Ins, Erweiterungs-Snap-Ins, Überwachungssteuerelemente, Tasks, Assistenten und Dokumentation zum Verwalten der Hardware-, Software- und Netzwerkkomponenten des Windows 2000-Systems enthält.

LDAP

Lightweight **D**irectory **A**ccess **P**rotocol. Das Internetprotokoll LDAP wurde zur Förderung des Verzeichnisstandards X.500 entwickelt, da sich das Originalprotokoll DAP (**D**irectory **A**ccess **P**rotocol) für die Internet Clients in der Benutzung als zu komplex erwiesen hatte. LDAP bietet einen Standard für die Kommunikation mit Datenbanken im Internet. So werden im Internet Zugriffe auf Verzeichnisdienste realisiert, um beispielsweise E-Mail-Adressen oder Zertifikate abfragen zu können. Durch Gateways ist es aber nicht mehr auf diesen einen Verzeichnisdienst festgelegt. Die Einträge sind als Objekte verpackt. Sie bestehen aus Attributen mit Typen und Werten und sind in einem hierarchischen Baum strukturiert. Objektklassen definieren, welche Attribute mit welchen Wertetypen erlaubt sind. Mögliche Typen sind unter anderem IA5- (ASCII) Zeichenketten, JPEG-Fotos, Sounddaten, URLs und Zertifikate.

LDIF

LDAP **D**ata **I**nterchange **F**ormat. LDIF wird in der Hauptsache für den Austausch von Adressdaten auf LDAP-Servern eingesetzt. LDIF ist ein textbasiertes Format (Ascii), welches leicht mit gewöhnlichen Editoren bearbeitet werden kann und auch von vielen E-Mail-Clients beim Im- und Export von Adressbüchern unterstützt wird (z.B. Outlook, Outlook-Express, Netscape, The Bat!).

Mailflooding

(Mailschwemme). Unter Mailflooding versteht man den Massenversand von E-Mails, die meistens von einer einzigen Domäne verschickt werden und im Abstand von wenigen Sekunden auf einem Mail-Server eingehen. Der Server wird durch diese "Attacken" in seiner Performance (Leistung) beeinträchtigt, da er in kurzer Zeit eine übergroße Anzahl von E-Mails verteilen muss. In der Regel handelt es sich bei solchen Mails um unerwünschte und unverlangte Post (siehe auch Spam) oder schlechte Scherze.

Makroviren

Lauern vor allem in Dokumenten der weitverbreiteten MS-Office Applikationen (wie Word, Excel, Access, Power Point). MS-Office Applikationen können über die Programmiersprache VBA gesteuert werden, die Makros benutzt. Auch HTML-Dokumente, die mit Word erstellt wurden, können Makroviren erhalten. Makroviren können sich sogar auf unterschiedlichen Betriebssystemen ausbreiten, da MS-Office das Makro interpretiert und dann ausführen kann.

Messagingplattformen

Hard- und Softwareplattformen für E-Mail bzw. elektronische Kommunikation.

MIME

Multi-purpose Internet Mail Extensions (.STM-Dateien). Ursprünglich eine Methode für die Verschlüsselung von Nicht-Texten, um deren Übertragung über SMTP und E-Mail zu ermöglichen. Diese Methode wird heute überall für andere Internet-Übertragungen verwendet und erweitert die Möglichkeiten von E-Mail durch die Definition spezieller Steuercodes zum Übertragen von Sonderzeichen wie zum Beispiel Umlauten und beliebiger Dateien als Anhang an Mails. Siehe auch S/MIME.

MMC (Microsoft Management Console)

Administrationsumgebung zur Verwaltung von Netzwerken, Rechnern, Diensten usw., das Verwaltungstools und Anwendungen enthält. Mit MMC können Sie Sammlungen von Tools und Anwendungen erstellen, speichern oder öffnen.

MMC Snap-In

Bestandteil (für Verwaltungsfunktionen) einer MMC (Microsoft Management Console), siehe Snap-In.

Modul

Eine nach Aufbau und Wirkung abgrenzbare programmtechnische Einheit, die als unabhängiger und selbstständiger Programmbaustein in ein Gesamtsystem eingebettet ist, z.B. securiQ mit den Modulen Watchdog und iQ.Suite Wall.

Mounten

engl. wörtlich "empor- oder (auf)steigen". In der EDV wird damit das "Einhängen" eines Dateisystems (Laufwerk) in ein bereits laufendes Rechnersystem bezeichnet.

Objekt

Die grundlegende Einheit von Active Directory. Es handelt sich um eine definierte, benannte Attributmenge, die etwas Konkretes darstellt, beispielsweise einen Benutzer, einen Drucker, einen Computer oder eine Anwendung.

OEM

Original Equipment Manufacturer; Unternehmen, das Produkte oder Komponenten anderer Hersteller einkauft und diese unter eigenem Namen weiterverkauft bzw. in eigene Produkte integriert.

Öffentliche Ordner-Hierarchie

Eine Struktur oder Hierarchie Öffentlicher Ordner mit einem einzelnen Informationsspeicher für Öffentliche Ordner.

öffentlicher Schlüssel

Der öffentliche Schlüssel ist der Teil eines Schlüsselpaares, der öffentlich, z.B. auf einem Trustcenter (LDAP) Server, zugänglich gemacht wird. Er ist dazu da, Nachrichten an den Inhaber des öffentlichen Schlüssels zu verschlüsseln und von diesem getätigte digitale Signaturen zu überprüfen. Ein von einer CA beglaubigter öffentlicher Schlüssel heißt Zertifikat.

Organisationseinheit

Ein Active Directory-Container, in dem Objekte wie beispielsweise Benutzerkonten, Gruppen, Computer, Drucker, Anwendungen, Dateifreigaben und andere Organisationseinheiten gespeichert werden können. Organisationseinheiten können verwendet werden, um Gruppen von Objekten (beispielsweise Benutzern und Druckern) bestimmte Berechtigungen zuzuweisen und diese zu speichern. Eine Organisationseinheit kann keine Objekte aus anderen Domänen enthalten.

Eine Organisationseinheit ist die kleinste Einheit, der Sie Verwaltungsrechte zuweisen oder an die Sie diese delegieren können.

Outlook Web Access

Outlook Web Access für Microsoft Exchange 2000 Server bietet Benutzern den Zugriff auf E-Mail, persönliche Kalender, Gruppenzeitplanung, Kontakte und Anwendungen zur Zusammenarbeit über einen Webbrowser. Outlook Web Access kann für UNIX- und Macintosh-Benutzer, für Benutzer ohne Zugriff auf einen Outlook 2000-Client oder für Benutzer eingesetzt werden, die die Verbindung aus dem Internet herstellen. Outlook Web Access bietet plattformübergreifenden Zugriff für servergespeicherte Benutzer, für Benutzer mit beschränkten Hardwareressourcen und für Benutzer, die keinen Zugriff auf ihre eigenen Computer besitzen.

Packer

sind Komprimierungsprogramme, siehe Komprimierung.

Passphrase

Eine lange, aber einprägsame Zeichenfolge (wie z.B. kurze Sätze mit Interpunktion), die das Passwort ersetzen sollten, da sie sicherer sind.

Passwort

Eine geheime Zeichenkette, deren Kenntnis als der Ersatz für die Authentifizierung eines Teilnehmers dienen soll. Üblicherweise ist ein Passwort zu kurz, um wirklich die Sicherheit zu gewährleisten, dass ein Angreifer es nicht durch Ausprobieren erraten kann.

PGP

Steht für Pretty Good Privacy und ist ein Programm zur Verschlüsselung und Entschlüsselung von E-Mails. Außerdem können Dokumente mit einer elektronischen Unterschrift versehen werden. Der Empfänger eines solchen Dokumentes kann sich darauf verlassen, dass der Absender auch der Autor ist, und kein Dritter es versendet bzw. verändert hat. PGP ist Freeware und damit kostenlos über viele Shareware-Archive zu beziehen. Im E-Mail-Bereich ist PGP ein Standard wie S/MIME. PGP ist plattformunabhängig.

PKI

Public Key Infrastruktur. Das größte Problem beim Einsatz von Public Key-Verfahren stellt die Authentizität von öffentlichen Schlüsseln dar. Dahinter verbirgt sich die Frage, wie gewährleistet werden kann, dass der vorliegende Schlüssel wirklich vom gewünschten Kommunikationspartner stammt. Eine PKI ist eine Kombination aus Hardware- und Software-Komponenten, Policen und verschiedenen Prozeduren. Sie basiert hauptsächlich auf sogenannten Zertifikaten; diese sind ihrerseits durch digitale Signaturen von einer vertrauenswürdigen Instanz beglaubigte Schlüssel der Kommunikationspartner.

Plattform

Technologiebasis, z.B. Lotus Notes oder Microsoft Exchange (auch jedes Betriebssystem), auf der andere Technologien oder Prozesse wie die Produkte der GROUP Technologies AG (oder auch Anwendungen anderer Art) aufgesetzt werden können.

Policy

Sammelbegriff für alle definierten Jobs, siehe Richtlinien.

POP3

Abkürzung für Post Office Protocol 3 (die 3 steht für die Version des Protokolls). Es handelt sich hier um ein Übertragungsprotokoll, welches den E-Mail-Empfang von einem entfernten Server steuert, auf dem die Mails zwischengelagert werden, bis der Benutzer sie abholt. POP3 benutzt dazu eine TCP/IP-Verbindung. Das Protokoll wurde speziell für den Empfang von Mails entwickelt, da es im Gegensatz zu SMTP dafür keine Standleitung benötigt.

Postfachspeicher

Der Teil des Informationsspeichers, der Informationen in Benutzerpostfächern verwaltet. Ein Postfachspeicher setzt sich aus einer Rich-Text-Format (RTF)-Datei (.EDB-Datei) und einer systemeigenen Streaming-Internetinhaltdatei (.STM-Datei) zusammen.

Private Key

Siehe unter privater Schlüssel.

privater Schlüssel

Der private Schlüssel ist der Teil eines Schlüsselpaares, den ein Benutzer sicher verwahren muss. Er ist dazu da, Nachrichten an den Inhaber des privaten Schlüssels zu entschlüsseln und digitale Signaturen zu erzeugen. Geschützt wird der private Schlüssel durch ein Passwort oder eine Passphrase. Siehe auch öffentlicher Schlüssel.

Public Key

Siehe unter öffentlicher Schlüssel.

Quarantäne

Die Quarantäne ist ein Archivordner, in dem die infizierten und/oder verbotenen Dateien abgespeichert werden und jederzeit von einer autorisierten Person eingesehen werden können.

Regel

Regeln grenzen innerhalb des Jobs durch eine Abfrage die Anzahl der E-Mails oder Datenbanken ein, die durch die iQ.Suite geprüft werden sollen. Die Regeln filtern die Mails und Datenbanken nach firmeneigenen, selbst festzulegenden Richtlinien und ermöglichen so eine optimale Gewährleistung des firmeneigenen Sicherheitskonzeptes.

regelbasiert

Der Ablauf von elektronischen Prozessen bzw. Funktionen aufgrund bestimmter, vom Systemadministrator eingestellter Regeln.

Replikation

Datenabgleich bei zwei gleichen Datenbanken auf zwei verschiedenen Servern.

Reseller

Händler, die neben der eigentlichen Software überwiegend auch eigene Leistungen mit anbieten.

RFC 821

Abkürzung für Request for Comments. RFC 821 definiert das Übertragungsprotokoll SMTP und ist heute die Basis für den Transport von E-Mails im Internet. Dieser Standard wurde im Jahre 1982 in RFC 821 und RFC 822 festgehalten. RFC

822 definiert das Format einer E-Mail. Es gibt eine ganze Reihe von RFC-Dokumenten, die das IAB erstellt hat.

Rich-Text-Format (RTF)

Ein Standardformat zum Übertragen von formatierten Textdokumenten zwischen Anwendungen, sogar zwischen Anwendungen, die unter verschiedenen Betriebssystemen ausgeführt werden.

Richtlinien

Die Gesamtkonfiguration aller Jobs einer Firma bezeichnen wir als Richtlinien.

Root-Zertifikat

Oberste Instanz eines Zertifikats. Näheres siehe Zertifikat.

RSA

Häufig verwendetes Verschlüsselungsverfahren, das nach seinen Erfindern **R**ives, **S**hamir und **A**dleman benannt wurde. RSA wird unter anderem bei PGP verwendet. Bei der RSA-Verschlüsselung werden zwei große Primzahlen zu einer noch größeren Primzahl verknüpft. Und mit dieser Zahl wird dann verschlüsselt. Ab einer gewissen Bitbreite (ca. ab 100 Bit) ist diese Verschlüsselung selbst mit schnellsten Hochleistungsrechnern nicht mehr zu knacken, wobei sich der Aufwand mit jedem zusätzlichen Bit verdoppelt.

S/MIME

Secure Multipurpose Internet Mail Extensions. Bedeutet: eine sichere Version von MIME. S/MIME ist der Industriestandard für die Verschlüsselung von E-Mails, die zwischen gleichen und ungleichen E-Mail-Systemen versandt werden. S/MIME kann eine Reihe unterschiedlicher Signatur- und Verschlüsselungsalgorithmen verwenden. Siehe auch PGP.

Server

Zentrale Instanz (Hardware oder Anwendungen; in der Regel ein allgemein zugänglicher Computer), die einen bestimmten Dienst zur Verfügung stellt, der von den an das Netz angeschlossenen Arbeitsstationen (Clients) genutzt werden kann, siehe Client/Server-Systeme.

serverbasiert

Programme sind auf einem Server installiert und werden auch dort ausgeführt.

Shareware

Kunstwort aus share (teilen) und Software, auch oft als Trialware bezeichnet. Es handelt sich um Software, die von ihrem Entwickler zunächst zur Probe angeboten wird. Gefällt sie, ist an den Softwareautor ein Betrag (Registrierungsgebühr) zu entrichten. Man erhält dann eine Vollversion ohne eventuelle Funktionsbeschränkungen der Demoversion.

Skalierbarkeit

Die Anpassungsfähigkeit eines EDV-Systems an die Anforderungen eines Anwenders/Unternehmens hinsichtlich der Verarbeitungsgeschwindigkeit, der Speicherkapazitäten, der Anzahl und Art der angeschlossenen Arbeitsplätze.

SMTP

Abkürzung für Simple Mail Transfer Protocol zur TCP/IP-Familie gehörendes Übertragungsprotokoll nach RFC 821 für den E-Mail-Empfang und -Versand. SMTP-Nachrichten bestehen aus einem Kopf, der mindestens die Kennungen des Senders und des Empfängers enthält, und der eigentlichen Nachricht. Die vom Absender verfasste Nachricht wird mittels eines E-Mail-Programms, dem User Agent (UA) an den dafür bereitgestellten Server im eigenen Netzwerk, den Message Transfer Agent (MTA) weitergereicht. Dieser reicht wiederum nach dem "Store and Forward-Prinzip" (speichern und weitergeben) die E-Mail an die auf dem Versandweg liegenden MTA's weiter, bis die Nachricht ihren Empfänger erreicht. SMTP arbeitet mit dem 7Bit-ASCII, die einwandfreie Darstellung von Umlauten ist daher ebenso nicht gewährleistet wie der Schutz vor unbefugtem Zugriff. ESMTP überträgt dagegen 8 Bits. Für den Empfang benötigt SMTP im Gegensatz zum Post-Office-Protocol (POP3) eine Standleitung.

Snap-In

Software, die die kleinste Einheit einer MMC (Microsoft Management Console)-Erweiterung darstellt. Ein Snap-In stellt eine Einheit von Verwaltungsverhalten dar. Der Systemmanager ist ein Exchange-Snap-In in MMC.

SOAP

(Simple Object Access Protocol) Setzt auf XML auf und dient als gemeinsame Sprache zur Abwicklung von Transaktionen. SOAP stellt für Applikationen eine Möglichkeit zur Verfügung, untereinander unabhängig von der Plattform über das

Internet zu kommunizieren. SOAP erlaubt z.B. die Auslösung einer Warenbestellung, ohne den eigentlichen Aufbau des Zielsystems zu kennen.

Spam

Unverlangte E-Mails, die in der Regel an einen großen Verteiler gehen, z.B. Werbemails, siehe auch Junk-Mail.

Speichergruppe (Storage Group)

Gruppe von Exchange Stores. Eine Zusammenstellung von Postfachspeichern und Informationsspeicher für Öffentliche Ordner, die eine Sammlung von Transaktionsprotokolldateien gemeinsam verwendet. Exchange verwaltet jede Speichergruppe mit einem separaten Serverprozess.

SSL

Secure Socket Layer - eine von Netscape entwickelte Methode für die sichere Übertragung von Daten im Netz. Mit Hilfe von SSL können die Daten verschlüsselt übertragen (RSA-Verschlüsselung) und so vor Fremdzugriffen geschützt werden. Wird zum Beispiel für die Übertragung von Kreditkartennummern benutzt.

Suite

Logische Einheit von Programmen eines Herstellers für ein bestimmtes Aufgabenfeld, z.B. E-Business-Security.

symmetrisches Verfahren

In diesem Fall werden die Mails mit demselben Schlüssel entschlüsselt wie verschlüsselt. Da die Schlüssel gleich sind, wird das Verfahren symmetrisch genannt. Das bedeutet, dass sowohl dem Absender als auch dem Empfänger der Schlüssel bekannt sein muss. Der Schlüsselaustausch zwischen Empfänger und Absender wird mit einer passwortgeschützten Schlüsseldatei vollzogen. Der Empfänger einer E-Mail bekommt das Passwort für die Schlüsseldatei vom Absender auf alternativem Weg, also z.B. auf einer „abhörsicheren Leitung“ mitgeteilt und kann die Mail dann entschlüsseln.

Systemarchitektur

Aufbau eines IT-Systems, bestehend aus Hardware- und Softwarekomponenten.

Systemintegratoren

Anbieter, die Hard- und Softwareprodukte verschiedener Hersteller sowie eigene Komponenten in reibungslos funktionierende Lösungen integrieren.

TCP

Abkürzung für Transmission Control Protocol. Neben IP (siehe IP-Adresse)das zentrale Protokoll in der Internet Protokoll Suite. Es stellt den Applikationen einen verbindungsorientierten, zuverlässigen Duplexdienst in Form eines Datenstroms zur Verfügung.

TCP/IP

Zusammensetzung aus TCP und IP (Abkürzung für Transmission Control Protocol/Internet Protocol), wurde ursprünglich für Unix-Netze entwickelt und hat sich zum allgemeinen Netzwerkprotokoll des Internets entwickelt. Die Daten werden in handliche Pakete zerlegt und über das Netz geschickt. Den Weg finden sie mit der individuellen IP-Adresse (Internet Protocol-Adresse) des Zielcomputers. Dort setzt TCP die Daten wieder automatisch zusammen. Außerdem ist es möglich, auf einer einzigen Modem/ISDN-Leitung mehrere Internet-Anwendungen gleichzeitig zu betreiben.

Tools

Werkzeuge in Form kleinerer Programme, Hilfs- oder Zusatzsoftware unterschiedlichster Art.

Trustcenter

Ein Trustcenter ist ein meist kommerzieller Dienstleister, z.B. unter http://www.d-trust.net/, der öffentliche Schlüssel ausstellt, verwaltet und bereitstellt. In der Regel unterteilt man die Aufgabenbereiche eines Trustcenters in drei verschiedene Bereiche: - die eigentliche Zertifizierungsstelle (CA) übernimmt die eigentliche Beglaubigung der vorliegenden Informationen, - die Registrierungsstelle (RA (Registration Authority)), ist für die Identifikation der Teilnehmer und die Übergabe der Zertifikate zuständig, - der Verzeichnisdienst stellt die zur Erstellung und zur Überprüfung ausgestellter Zertifikate und Signaturen notwendigen Informationen (wie z.B. Zeitstempel oder CRLs) zur Verfügung.

Universal Naming Convention (UNC)

Eine Konvention zur Benennung von Dateien und anderen Ressourcen, bei der ein Name mit zwei umgekehrten Schrägstrichen (\) beginnt, um zu kennzeichnen, dass die Ressource auf einem Netzwerkcomputer vorliegt. UNC-NAmen weisen die Syntax \\Servername\Freigabename auf.

Unterstützte Anwendungen

Handelsübliche Programme und Tools (WinZip, Sophos-Virenscanner, PGP usw.).

VBA

Visual Basic for Applications. Mit dieser Programmiersprache von Microsoft lassen sich z.B. MS-Office Programme wie Word, Access oder Excel steuern.

Verschlüsselung

Eine Nachricht (durch Chiffrieren) unkenntlich machen, um sie davor zu schützen, von Unbefugten gelesen zu werden. Es gibt unterschiedlich komplexe Verschlüsselungsverfahren. Siehe auch PGP und S/MIME.

vertrauende Domäne

Eine Domäne, die einer anderen vertraut. Diese Domäne vergibt Rechte an die vertraute Domäne und gewährt Benutzern aus diesen vertrauten Domänen Zugriff auf ihre Ressourcen.

vertraute Domäne

Eine Domäne, der vertraut wird. Benutzer in vertrauten Domänen können bei Berechtigung z.B. in einer vertrauende Domäne auf die Ressourcen zuzugreifen oder mit Benutzerrechten ausgestattet werden.

Virenscanner

Programm zur Identifizierung eines Virus.

Virus

Ein Virus ist Code, der von einer Datei oder einem Objekt zum anderen springen kann. Ein Virus definiert sich durch seine Eigenschaft, sich selbst zu reproduzieren. Viren können andere Programme infizieren, indem sie sich in eine ausführbare Datei einhängen oder den Bootsektor von Festplatten bzw. Disketten befallen.

VPN

Virtual **P**rivate **N**etwork. Ein VPN ist ein Netz, das seine Knotenpunkte über öffentliche Netze (z.B. Internet) verbindet. Durch den Einsatz kryptographischer Verfahren kann alle Kommunikation vertraulich (daher virtuell private) durchgeführt werden.

Web

Synonym für Internet, wobei der Aspekt des weltumspannenden Informationsnetzes im Vordergrund steht.

Web Storage System

Webbasierter Informationsspeicher, der Zugriff auf unterschiedlichste Informationen bietet, z.B. E-Mail oder Multimedia-Dateien. Das Web-Store-Konzept verknüpft Messaging, den Zugriff auf Dateien und Exchange Datenbankfunktionen (z.B. multiple Datenbanken und Transaktionsprotokollierung). Der Web Store ist die Technologie, die in den Exchange 2000 Informationsspeicher eingebettet ist, und eine logische Sicht auf die physischen Datenbanken zur Verfügung stellt. Siehe auch Informationsspeicher und Installierbares Dateisystem.

Webconnect

Anschluss an das Internet.

Wildcard

Ein Platzhalter, der einzelne Zeichen oder ganze Zeichenfolgen ersetzt. Am bekanntesten sind die vom DOS-Kommandointerpreter benutzten Wildcards ? und *. Das Fragezeichen (?) ersetzt einzelne Bu??staben und Zahl?n. Der Stern (*) ersetzt bis zum Wortende alle restlichen Buchst* und Zahl*.

Wissensmanagementsystem

System, in dem ein Unternehmen Wissen sammelt, organisiert, teilt und analysiert, um seine Ziele zu unterstützen.

Wurm

Ein selbst ausführbares Programm, welches sich vermehren kann. Würmer benötigen keine Containerdatei (.com, .exe oder Visual Basic innerhalb eines Dokuments) wie ein Virus, um sich zu verbreiten. Sind häufig als Makroviren anzutreffen.

X.509

Standard für den Aufbau und die Codierung von Zertifikaten, CRLs und Authentifizierungsdiensten. X.509 ist die weltweit am häufigsten eingesetzte Norm für Zertifikatsstrukturen.

XML (Extensible Markup Language)

Metasprache zur Definition von Markup-Sprachen (z.B. HTML).

Zertifikat

Ein digitales Zertifikat ist ein elektronisches Dokument, das mit dem öffentlichen Schlüssel verbunden ist. Ein Zertifikat wird durch eine vertrauenswürdige Instanz (Zertifizierungsstelle/Trustcenter, siehe auch PKI) digital signiert und damit beglaubigt, dass der Schlüssel z.B. zu einer bestimmten Person gehört und nicht verändert wurde. Die digitale Signatur der Zertifizierungsstelle ist dabei integraler Bestandteil des ausgestellten Zertifikats. So kann jeder Teilnehmer, der den öffentlichen Schlüssel dieser Zertifizierungsstelle kennt, deren Zertifikate überprüfen. Durch eine mehrstufige Anwendung dieser Methode entsteht eine Public-Key-Infrastruktur (PKI). Vorteile solcher Vorgehensweisen sind, dass man zur vollständigen Prüfung nur noch den öffentlichen Schlüssel der sogenannten Root-Instanz, also das Root-Zertifikat benötigt und die Überprüfung der Zwischenzertifikate automatisch erfolgt. Siehe auch öffentlicher Schlüssel und privater Schlüssel.

Zertifizierungsstelle

Auch Zertifizierungsinstanz oder Certification Authority (CA). Die CA, im deutschen auch Zertifizierungsstelle genannt, ist eine vertrauenswürdige Instanz mit der Aufgabe der Beglaubigung von kryptographischen Schlüsseln (siehe Zertifikat). Sie ist Bestandteil einer PKI. Eine Zertifizierungsstelle (CA) stellt Zertifikate aus. Sie bestätigt durch ihre digitale Signatur die Richtigkeit der im Zertifikat vorhandenen Daten. Üblicherweise sind dies der Name des Schlüsselinhabers sowie weitere ihn identifizierende Attribute, der öffentliche Schlüssel des Schlüsselinhabers, seine Gültigkeitsdauer sowie der Name der Zertifizierungsstelle. Der Grad des Vertrauens in ein solches Zertifikat hängt von den operativen Verfahrensweisen der Zertifizierungsstelle ab, also etwa davon, wie sie die Identität eines Schlüsselinhabers prüft. Nach der Ausstellung eines Zertifikats muss die Zertifizierungsstelle die Möglichkeit bieten, das Zertifikat wieder zu sperren und

dafür Sperrlisten (CRLs) bereitstellen, sofern Angaben im Zertifikat ungültig werden. Dies gilt insbesondere dann, wenn private Schlüssel des Schlüsselinhabers kompromittiert wurden. Siehe dazu auch öffentlicher Schlüssel und privater Schlüssel.

ZIP of Death

ZIP of Death sind rekursiv gepackte ZIP-Dateien, deren Name von einer unscheinbaren 42KB großen E-Mail stammt, die als solche ungefährlich und auch kein Virus ist. Dahinter verbirgt sich aber ein wahrhaft riesenhaftes ZIP-Gebäude von mehr als einer Million Dateien und einer ausgepackten Gesamtgröße von 49.000.000 Gigabytes. Diese unscheinbare Mail zwingt den Entpacker eines Virenscanners in uferlose Endlosschleifen. Die Folge ist meist ein Absturz. Davon betroffen sind nicht nur die kleinen Virenscanner der Arbeitsplatzrechner, sondern auch die Mailserver, die innerhalb von wenigen Minuten abstürzen können und somit den E-Mail-Verkehr zum Erliegen bringen.

Index

A

Active Directory 75
Adressen
    Bei mehreren Empfängern jeden einzeln verarbeiten 94
    Wildcards 267
Adresslisten
    ändern 92
    anlegen 90
    Einsatz im Job 93
    löschen 92
Adressprüfung
    Ablauf 266
    Absender und Empfänger 268
    Aktionen 270
    Objekte 266
Aktionen 121
Anhanggröße
    Aktionen 263
    einschränken 260
    gültig für 260
    komprimierte Anhänge 262
Anti-Spam 281
    Aktionen 283, 290
    Konfiguration 288
    Praxistipps 287
    Schwellwerte 302
    Spam-Wahrscheinlichkeit 302
AntiVir
    Installation 25
    Konfiguration 219
Anzahl der Empfänger 322
    Aktionen 324
    festlegen 324
Anzahl der Threads 86, 218
Archive
    Entpacke komprimierte Anhänge 254
    Entpackungstiefe 20, 77
    Formate 76
    maximale Größe entpackter Dateien 20

Obergrenze für entpackte Dateien 77
Authentizität 330

B

Bad-Mails 132
Basis-Konfiguration 85
Bei mehreren Empfängern jeden einzeln verarbeiten (Split) 94
Benachrichtigungsvorlagen
erstellen 100
Platzhalter 101
vorkonfigurierte 101
Benutzer-Quarantäne 87
Quarantänezugriff per HTTP-Anfrage ermöglichen 89
Quarantänezugriff per Mail-Anfrage ermöglichen 88

C

CA 331
CORE
anlernen 132
Anti-Spam 313
Inhalte klassifizieren 315
Klassifikator trainieren 313
Klassifizierung aus Quarantäne 126
kombiniertes Kriterium 304
Übersicht 312
CRL 331

D

Dateieinschränkungen
Ablauf 241
Aktionen 242, 255
Fingerprint-Bedingungen 254
Fingerprints auswählen 253
nach E-Mail-Größe 242
nach Typ 241
nachTyp und/oder Anhanggröße 243
DCC
Einstellungen 310
Jobbeispiel 312
kombiniertes Kriterium 304
Konfiguration 309
Server 309, 310
Übersicht 307

Deinstallation 38
Domäne
    Einstellungen 20
    interne 21

E

EICAR Test Virus 23
E-Mail-Adressen
    Definition 87
    einrichten 87
E-Mail-Größe
    Aktionen 259
    festlegen 258
    gültig für 257
EMH 73, 80
Entferne S/MIME Signatur 184
Entpacker 76
Exchange SCL Wert 293
    definitives Kriterium 286
    kombiniertes Kriterium 304
Extrahiere reinen Nachrichtentext 155

F

Fingerprints
    Ausnahmen 255, 263
    Beispiel Windows/OS2 Bitmap 249
    Binärmuster anfordern 251
    Binärmuster anlegen 247
    Fingerprintkategorie 244
    Fingerprintkategorie anlegen 245
    konfigurieren 243
    Löschen 244
    Namensmuster anlegen 245
    Prüfe Binär- und Namensmuster 245

G

GrpData-Verzeichnis 26

H

Haftungsausschluss
    Adressierung 198
    anhängen 196

I

Importieren
    Basis-Objekte 85
Informationsspeicher
    Ersetzen 215
    Hintergrund Scan 214
    Nicht als virulent markieren 215
    Objekt blocken 215
    On-Demand Scan 214
    Proaktiver Scan 214
Informationsspeicher-Scan 214
Inhaltsprüfung
    Ablauf 271
    Aktionen 268
    Wortlisten 277
Installation 25
    auf dem Exchange-Server 27
    auf mehreren Exchange-Servern 31
    im Cluster 38
    Konsole auf der Workstation 36
    Systemvoraussetzungen 25
    Virenscanner 25
    Vorbereitungen 25
Interne Domäne 21
iQ.Suite
    Architektur 71
    beenden 17
    Benutzeroberfläche 80
    Crypt 135
    Domäne
        Eigenschaften 20
    Einstellungen für alle Server 22
    E-Mail-Verarbeitung 79
    Grabber 72, 79
    Icons 81
    Konsole 71
    Menüleiste 81
    Monitor 123
        Zugriffsberechtigung 75, 123
    Queue 77
    Reports 133
    Richtlinien-Konfiguration 118

Server 72
Eigenschaften 85
neuer Server 85
Service 73
Standardeinstellungen 87
starten 17
Trailer 193
Wall 265
Watchdog 211

J

Jobs
duplizieren 322
Liste 90
Jobtypen 118
Aktionen 121
Crypt 136
Trailer 193
Wall 265
Watchdog 211

K

Konfiguration
abweichend vom Standard 79
Anti-Spam manuell 306
Architektur 78
Basis 85
bei Installation beibehalten 37
importieren 85
Management Konsole 84
Speichern 17

L

Label 125
LDAP Server 168, 170, 172
LDIF 75

M

Mail umleiten 231

P

PGP
Ablauf der Verarbeitung 139
Entschlüsselung

Ablauf der Verarbeitung 161
Aktionen 166
Crypt Engine 163
Voraussetzungen 161
Extrahiere reinen Nachrichtentext 155
Fingerprints 144, 155
Key ID-Zuordnung 158
Konfiguration 140
Quickstart 137
Schlüssel importieren 146
Ablauf der Verarbeitung 146
Aktionen 149
Allgemeines 147
Optionen 148
Schlüssel unterschreiben 140
Variablen 145
Verschlüsselung
Ablauf der Verarbeitung 151
Aktionen 159
Crypt Engine 153
Crypt Modus 155
Mapping 158
Voraussetzungen 151
Versionskontrolle 149
Vorbereitungen 140
PKI 343
Priorität 120, 122
Vergabe 122

Q

Quarantäne
Arbeitsweise 74
aus Quarantäne senden 130
benutzerspezifischer Zugriff 87
CORE Klassifikation 126
E-Mail erneut durch iQ.Suite Jobs bearbeiten lassen 132
Filteroptionen 124
Icons 125
Informationsspeicher
Icons 129
konfigurieren 110
Kopie in Quarantäne 110, 124
Neue Quarantäne 111

Wartung 89
Zugriffsberechtigung 123
Zustellen ohne weitere iQ.Suite Prüfung dieses Servers 131

R

Registry 76
Richtlinien-Konfiguration 118
Root-Zertifikat 167, 169, 345

S

S/MIME
Entferne Signatur 184
Entschlüsselung
Ablauf der Verarbeitung 181
Aktionen 186
Crypt Engine 183
LDAP Server 170, 172
Quickstart 138
Signatur prüfen 189
Signieren 187
Ablauf der Verarbeitung 188
Verifizieren
Ablauf der Verarbeitung 189
Verschlüsselung
Aktionen 180
Crypt Engine 174
Crypt Modus 176
Mapping 179
Vorbereitungen 167
Zertifikate importieren 189
Schreibe Spam-Ergebnis in Exchange SCL Feld 293
Schreibe Spam-Ergebnis in Mail-Header 294
Server
Eigenschaften 85
E-Mail-Adressen 87
neuer Server 85
Server Status 239
Sicherheitswarnung 28
Signatur
anhängen 202
anlegen 203
Sonderzeichen 279
Spam manuell blocken 306

Spam-Wahrscheinlichkeit 302
Split 94
Statistik 133

T

Textbaustein
  anhängen 194
  anlegen 194
Textprüfung
  Aktionen 280
  Schwellwert 277, 278
  Sonderzeichen 279
  Verschiedene Sprachen 279
  Zeichenumsetzung 279
TNEF-Format 154, 231
Trailer
  anlegen 194
  aus Job entfernen 199
  auswählen 198
  Signatur anlegen 203
Trustcenter 348

U

Unternehmensrichtlinie 93, 96, 118
Unternehmens-Zertifikat 167, 169, 188
Update auf Version 5 26

V

Variablen 101
  Tokens 110
Virenprüfung
  Aktionen 213
  Aktionen festlegen 228
  gepackte Dateien extra prüfen 229
  Informationsspeicher-Scan 214
  Prüfen Nachrichtentext 230
Virenscanner
  aktivieren 22
  auswählen 226
  Command Software Scan Engine 221
  F-Secure Scan Engine 221
  H+BEDV Scan Engine 219
  installieren 25

konfigurieren 216
McAfee Scan Engine 221
Norman Scan Engine 222
Optionen 218
Parameter 217
Sophos Scan Engine (SAVI) 223
Symantec Scan Engine 223
Test 23
Trend Micro Scan Engine 223
Update-Einstellungen 218
VPN-Kanäle 155, 164

W

Wildcards in Adressen 267
Wildcards in Wortlisten 272
Wortlisten
anlegen 272
auswählen 277
Schwellwert 274, 277, 278
Wertigkeit 272, 278
Wildcards 272

X

X.509 Zertifikate 167
X-Header-Feld 121, 294, 310

Z

Zeichenumsetzung 279
Zertifikat 351

Notizen